Manual de Procedimientos, Recomendaciones y Formularios

Ministerio de Gobierno y Reforma del Estado
Secretaría de Tecnologías para la Gestión
Junio de 2010

Índice

Introducción....3
Ambito de Aplicación....3
Alcance....3
Autoridad de Certificación....3
Autoridad de Registro....3
Contactos....3
PROCEDIMIENTOS....4
Procedimiento Nº 1 – Incorporar Firma Digital en un Circuito de la Administración ...5
Procedimiento Nº 2 - Solicitar un Certificado Digital de Clave Pública....8
Procedimiento Nº 3 – Revocar un Certificado de Clave Pública....12
Procedimiento Nº 4 – Renovar un Certificado de Clave Pública....14
Procedimiento Nº 5 – Préstamo de Dispositivos Criptográficos 15
Procedimiento Nº 6 – Gestión de Certificados de Clave Pública....17
Procedimiento Nº 7 – Configuración de Cliente de Correo Electrónico 20
Procedimiento Nº 8 – Envío de Correos Electrónicos Firmados Digitalmente....30
Procedimiento Nº 9 – Recepción de Correos Electrónicos Firmados Digitalmente....32
Procedimiento Nº 10 - Guía de Instalación y Administración del Token ePass 2000 36
Procedimiento Nº 11 - Guía de Instalación y Administración del Token ikey 2032...40
RECOMENDACIONES....45
Recomendación Nº 1 – Especificación Mínima para Dispositivo Criptográfico (Token) 46
Recomendación Nº 2 - Configuración Mínima de Equipo para Operar con Firma Digital....47
Recomendación Nº 3 - Aspectos de Seguridad Mínimos del Equipo de Trabajo....48
FORMULARIOS....49
Formulario Nº 1 – Jurisdicción y Responsables del Circuito Propuesto 50
Formulario Nº 2 – Descripción del Circuito Actual....51
Formulario Nº 3 – Documentos Involucrados en el Circuito 52
Instrucciones para completar el Formulario Nº 3....53
Formulario Nº 4 – Descripción del Circuito Modificado con Firma Digital 54
Formulario Nº 5 – Análisis de Factibilidad Técnica 55
Formulario Nº 6 – Detalle de Agentes Autorizados a Utilizar Firma Digital....56
Formulario Nº 7 – Solicitud de Revocación de un Certificado Digital....57
Formulario Nº 8 – Solicitud de Dispositivo Criptográfico 58
Formulario Nº 9 – Acta de Compromiso – Préstamo de Token....59
Formulario Nº 10 – Registro de Compras de Dispositivos Criptográficos....60
Formulario Nº 11 – Acta Compromiso – Area de Recursos Humanos 61
Formulario Nº 12 – Constancia de la Condición de Empleado de una Repartición ...62
Formulario Nº 13 – Solicitud de Actividad de Difusión de Firma Digital....63
Formulario Nº 14 – Recepción De Token....64
Formulario Nº 15 – Solicitud de Alta de Agente al Sistema SiCAP....65

Introducción

El presente manual es una recopilación de los procedimientos, formularios y recomendaciones, elaborados por la Infraestructura de Firma Digital con el objetivo de coordinar las actividades de aplicación de la tecnología de clave pública.

Ambito de Aplicación

Poder Ejecutivo Provincial.

Alcance

Para la aplicación de esta tecnología se han definido etapas, de manera que la implementación se realice en forma gradual, a saber:

1. Utilización en procesos de notificaciones de documentación firmada digitalmente con correo electrónico también firmado digitalmente. Esta primera etapa, comprende aquellos circuitos de la administración, que hayan presentado un proyecto y que el mismo haya sido aprobado, de acuerdo al procedimiento que se indica en el presente documento.
2. Utilización con otro software de aplicación.
3. Extensión a otros ámbitos administrativos distintos al Poder Ejecutivo Provincial, como por ejemplo, para intercambio de información con otros poderes del Gobierno Provincial, Gobiernos Municipales y Nacional.
4. Interacción con los cuidadanos.

Actualmente, la etapa en consideración es la Etapa 1.

Autoridad de Certificación

Oficina Nacional de Tecnologías de Información (ONTI), de la Secretaría de la Gestión Pública dependiente de la Jefatura de Gabiente de Ministros.

Autoridad de Registro

Dirección General de Recursos Humanos de la Provincia, dependiente del Ministerio de Economía del Gobierno de la Provincia de Santa Fe.

Contactos

- Autoridad de Registro (AR):
  Dirección General de Recursos Humanos - Ministerio de Economía
  Centro Cívico: Av. Illía 1151 – 1º Piso
  Teléfono: 4506600 - int. 2694
  correo electrónico: arfirmadigital@santafe.gov.ar
- Infraestructura de Firma digital – Santa Fé (IFD-SF):
  Dirección Provincial de Gobierno Digital
  Secretaría de Tecnologías para la Gestión
  San Martín 2466 – 6º Piso
  Teléfono: 4508700 – int. 5143, 5220
  correo electrónico: firmadigital@santafe.gov.ar

PROCEDIMIENTOS

Procedimiento Nº 1 – Incorporar Firma Digital en un Circuito de la Administración

Este procedimiento se aplica cuando un área del Poder Ejecutivo Provincial considera apropiado y/o necesario incorporar firma digital en algún circuito administrativo con el objetivo de mejorar el proceso o parte de él, mediante la aplicación de esta tecnología.

Las propuestas de aplicación de firma digital sobre un circuito, se deberían presentar cuando se verifiquen alguna o todas las siguientes condiciones:

- El proceso requiere garantizar autoría y/o integridad sobre la información que se intercambia de forma digital.
- Se estima que la incorporación de firma digital producirá una reducción considerable de papel, tiempos y/o afectación de personal a las tareas involucradas.

El presente procedimiento se inicia con la presentación de una propuesta por parte de la jurisdicción o área solicitante, siempre a través de su área informática, y culmina con la aplicación de la tecnología en el/los circuitos seleccionados.

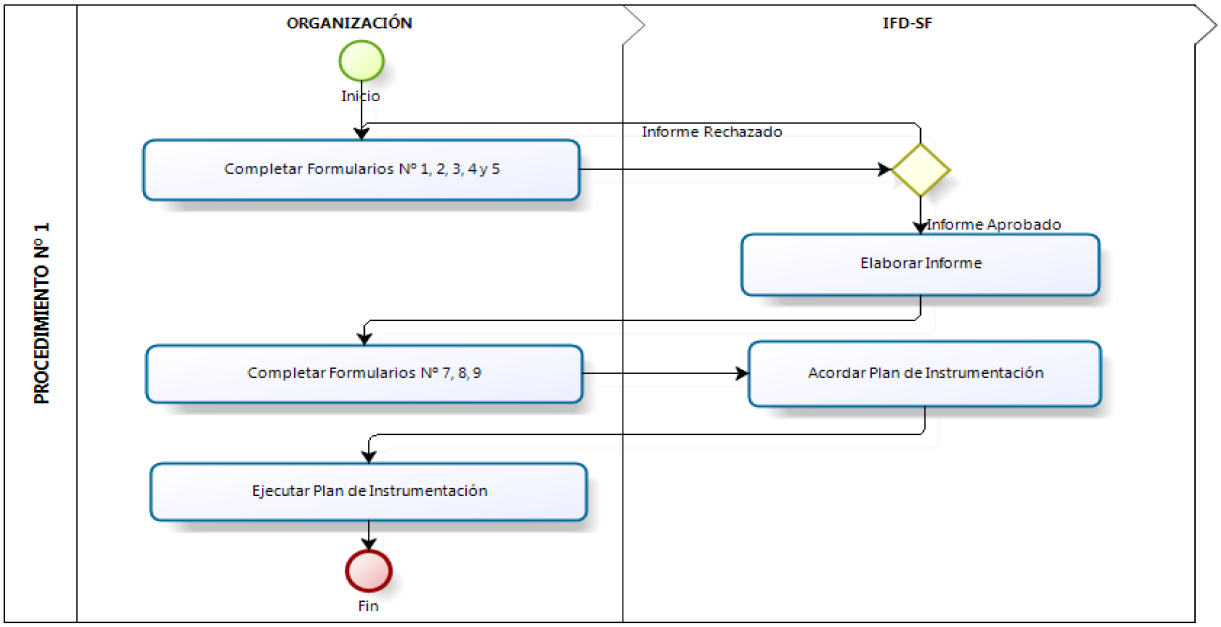
Este procedimiento tiene los siguientes objetivos para el área de aplicación:

- Identificar escenarios típicos de aplicación ó variables particulares de la jurisdicción.
- Valorar las variables identificadas, conjuntamente con los aspectos legales involucrados en los circuitos sobre los que se pretende aplicar firma digital.
- Realizar un análisis de costos, beneficios y riesgos.
- Elaborar el plan de implementación para el circuito propuesto.

Por otra parte, a la Secretaría de Tecnologías para la Gestión le permitirá:

- Medir impacto y resultados.
- Analizar y documentar soluciones técnicas y jurídicas.
- Elaborar recomendaciones y fijar estándares.

Descripción del Procedimiento



EN LA JURISDICCION

La jurisdicción deberá iniciar un trámite, a través de su correspondiente Sectorial de Informática, que será remitido a la Infraestructura de Firma Digital en la Dirección Provincial de Gobierno Digital. En el mismo, se deberá presentar la documentación que a continuación se detalla, completando los formularios correspondientes.

- **Formulario Nº 1 - Jurisdicción y Responsables del Circuito Propuesto**

La jurisdicción debe designar un responsable técnico del proyecto que sea personal de la Sectorial de Informática correspondiente. También debe designar el responsable del proceso o circuito de aplicación de firma digital, que será un funcionario o personal administrativo. Con estos datos se completa el Formulario N° 1, para brindar la información relativa al área donde se encuentra el proceso propuesto, responsables y datos de contacto.

- **Formulario Nº 2 - Descripción del Circuito Actual**

Se solicita realizar la descripción del circuito actual al que se quiere aplicar firma digital, para lo cual se muestra un esquema de presentación (Formulario Nº 2), que se divide en dos partes. Una primera parte, para detallar las funciones de las áreas involucradas en el proceso, incluso los roles de las personas que participan directa o indirectamente y normativa asociada. En la última columna se indica la normativa que podría regular en parte o totalmente el proceso.
La segunda parte, muestra un diagrama ejemplo que permite ver el flujo de la información en un proceso, según la participación de las diferentes áreas.

- **Formulario Nº 3 - Documentos involucrados en el Circuito**

En este punto se solicita describir la información que fluye por el proceso, la cual puede encontrarse en documentos internos o externos y volcar esta información en el Formulario Nº 3. Por ejemplo, podrían ser planillas, solicitudes, partes diarios, listados, etc., generados en forma manual o electrónica, que pueden provenir de fuentes propias o externas, pero que involucran información necesaria para completar el circuito en cuestión.
Para cada documento, se solicita indicar variables de tiempo, papel, aspectos relativos a la distribución y cualquier otro dato que se considere de interés para medir antes y después de la aplicación de firma digital al circuito, como por ejemplo, se podría incluir cantidad de personas afectadas a una tarea, costos asociados, etc.
Se solicita detallar todos los documentos que involucra el circuito, aún los que no se firmarán digitalmente e incluso aquellos que actualmente no llevan firma hológrafa, en lo posible asociar una copia del comprobante impreso.

- **Formulario Nº 4 - Descripción del Circuito modificado con Firma Digital**

Análogamente a lo presentado en el Formulario Nº 2, se solicita elaborar el diagrama de proceso con el circuito modificado por la aplicación de firma y reflejarlo en el Formulario Nº 4.
Es importante aclarar que aquí, se deberá indicar la normativa que a criterio de la jurisdicción, deberá adecuarse o generarse para validar el nuevo circuito.

- **Formulario Nº 5 - Análisis de Factibilidad Técnica**

Este análisis se realiza con el objetivo de medir qué beneficios aporta la aplicación de firma digital en el circuito propuesto. Se solicita la definición de variables de medición para el proceso, para reflejar el impacto de la aplicación de firma digital.

EN LA INFRAESTRUCTURA DE FIRMA DIGITAL

Se realiza la evaluación de la documentación presentada. Esta instancia implica un trabajo de intercambio de información con el área solicitante, que incluso podría involucrar aspectos de difusión en el área, con el fin de esclarecer los conceptos sobre la aplicación de la tecnología.
En esta etapa del proceso, el equipo de la Infraestructura de Firma Digital, con la colaboración de la jurisdicción y/o Sectorial de Informática, debe realizar las siguientes tareas:

- Análisis de la Normativa involucrada
- Análisis de la infraestructura de hardware y software del circuito propuesto
- Identificación de riesgos para la implantación de esta tecnología.

- Análisis de costos y beneficios.
- Elaboración de informe final, el cual puede tener estado rechazado o aprobado.

- **Informe Rechazado**

Si se emite un informe por el cual se rechaza un proyecto, podría suceder que la Infraestructura de Firma Digital sugiera una modificación al mismo y se reelabore una nueva propuesta.

También el rechazo podría dar lugar a un análisis de otros circuitos factibles de aplicación de firma digital en forma conjunta con la jurisdicción.

En cualquiera de las dos situaciones, se deberá generar una nueva propuesta.

- **Informe Aprobado**

En caso de aprobación, la Infraestructura de Firma Digital:

1) Notifica y envía la información correspondiente al responsable del proyecto, a través de correo electrónico firmado digitalmente.

2) Entrega un token al responsable del proyecto para que solicite un certificado digital y a partir de ese momento, realice el intercambio de información con la Infraestructura de Firma Digital a través de correo electrónico firmado digitalmente.

3) Instala la aplicación para firmar archivos pdf en la máquina del responsable del proyecto para poder enviar los documentos firmados digitalmente.

4) Conjuntamente con la jurisdicción se elabora un plan de instrumentación para ejecutar la aplicación de Firma Digital en el circuito propuesto, donde se indicarán:

- Etapas
- Tareas/Subtareas
- Tiempos previstos
- Recursos necesarios
- Roles y responsabilidades
- Circuito modificado (si corresponde)
- Resultados de cada etapa

EJECUCIÓN DEL PLAN

Para ejecutar el plan, se requiere:

- Que en la jurisdicción se hayan adquirido los dispositivos criptográficos o token que la Infraestructura de Firma Digital recomiende en esa oportunidad, para solicitar los certificados digitales de las personas involucradas en el proyecto (Recomendación Nº 1). Recordar que la Infraestructura de Firma Digital cuenta con un servicio de préstamo de tokens por un período limitado, hasta tanto la jurisdicción pueda adquirir los propios y restituirlos (ver Procedimiento Nº 5).
- Que la jurisdicción cuente con la infraestructura tecnológica y aspectos de seguridad recomendados (Recomendación Nº 2, Recomendación Nº 3).
- Que se brinden los datos de las personas autorizadas a firmar digitalmente al Sistema de Administración de Certificados, Agentes y Proyectos (SiCAP).
- Que la Sectorial de Informática de la jurisdicción involucrada cuente con la capacitación necesaria para brindar el asesoramiento y soporte que necesitan los usuarios para gestionar sus certificados digitales y operar con los mismos dentro del proyecto.

Procedimiento Nº 2 - Solicitar un Certificado Digital de Clave Pública

La solicitud de un certificado digital se debe realizar en el marco de un proyecto aprobado por la Infraestructura de Firma Digital. Esto significa que la jurisdicción o repartición a la que pertenece el solicitante debe haber cumplimentado lo establecido en el Procedimiento para Incorporar Firma Digital en un circuito de la Administración (Procedimiento Nº 1).

Para solicitar un certificado digital, es requisito lo siguiente:

- Que la Autoridad de Registro tenga registrado el apellido, nombre y número de documento del solicitante en un proyecto aprobado, información que es suministrada por Sistema de Administración de Certificados, Agentes y Proyectos (SiCAP).
- Contar con un dispositivo criptográfico (token) para almacenar la clave privada y los certificados de clave públicas necesarios.
- Contar con el equipamiento y el software necesario para poder utilizar esta tecnología.

Casos especiales

Organismos con Areas Propias de Recursos Humanos

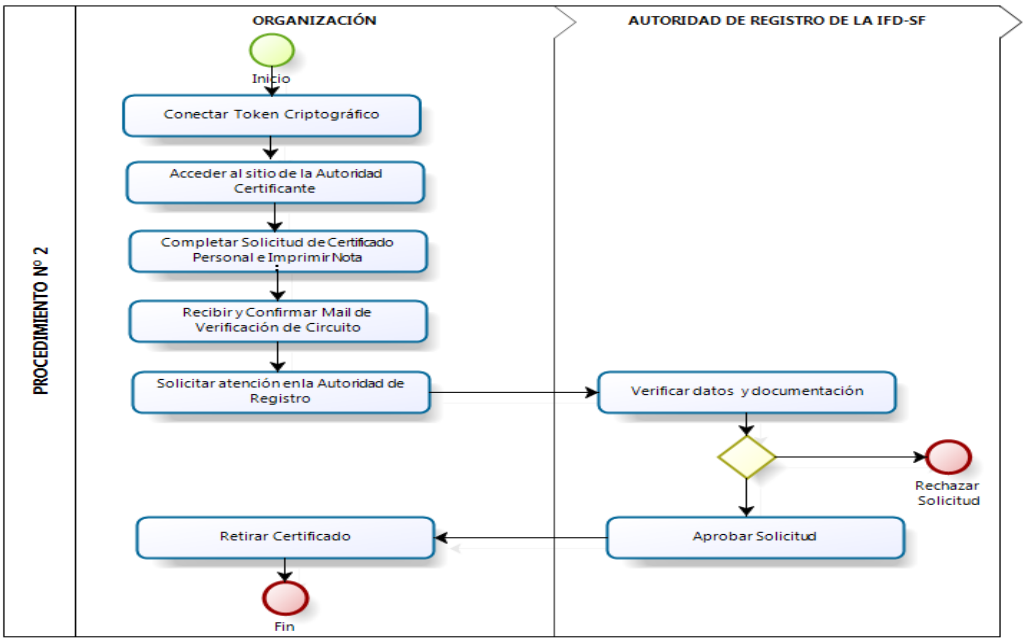
Aquellos organismos del Estado en los que la Dirección General de Recursos Humanos de la Provincia, no cuenta con la información referida al cargo y aspectos presupuestarios asociados, como por ejemplo, la Empresa Provincial de la Energía (E.P.E.) o el Ente Regulador de Servicios Sanitarios (ENRESS), cuentan con áreas propias de Recursos Humanos, que gestionan la información presupuestaria y de situación de revista del agente. En esta situación, previo a la solicitud de certificados digitales por parte de los agentes autorizados en cualquier proyecto, es requisito que el área de Personal o Recursos Humanos suscriba por única vez, un Acta Compromiso (Formulario Nº 11) ante la Autoridad de Registro, donde se compromete a informarle sobre cualquier modificación en la situación de los agentes de su organismo.

Luego, cada agente que se presente ante la Autoridad de Registro para acreditar su identidad en caso de haber solicitado un certificado digital, debe llevar el Formulario Nº 12, firmado por su responsable del Area de Recursos Humanos, donde conste su condición de empleado de la repartición.

Personal contratado o pasante

En todos los casos, el agente debe concurrir a la Autoridad de Registro con una constancia de la condición de empleado (Formulario Nº 12) firmado por una autoridad superior.

Descripción del Procedimiento



EN SU COMPUTADORA LOCAL

NOTA: Si bien el procedimiento se detalla para los navegadores Internet Explorer y Mozilla Firefox, debido a que con Internet Explorer se han presentado problemas varios recomendamos la utilización de Mozilla Firefox.

- Para solicitar un certificado de clave pública, se debe tener correctamente configurado y conectado el dispositivo de almacenamiento criptográfico (token).
- Se debe ingresar al sitio http://ca.pki.gob.ar, que es el sitio habilitado por la Autoridad Certificante (AC) de la Oficina Nacional de Tecnologías de Información.
- Presionar el enlace “Solicitar un Certificado Digital”. Luego, seleccionar “Alcance Otras Aplicaciones en el Ámbito de la Administración Pública”.
- Se presenta una nueva página con el título “Comunicaciones Internas en la Administración Pública”. Allí continúa con una serie de pasos a seguir para completar la solicitud del certificado digital. Se recomienda leerlos detenidamente e incluso, imprimir la página para realizar el seguimiento posterior. Por último, ingresar en opción Ir al Paso 1.
- **Paso 1** – Presenta la Política de Certificación de la Autoridad Certificante. Se debe prestar conformidad a la misma para poder continuar con el proceso.
- **Paso 2** – Instalación del certificado digital de la Autoridad Certificante en su navegador. Para ello, presionar el botón que indica esta instalación. Aparece una ventana donde se debe seleccionar la opción Abrir. Allí se muestra el certificado de la Autoridad Certificante y presenta en la parte inferior un botón “Instalar certificado...”. Presionarlo y una vez finalizada la instalación, utilizando el Asistente que se presenta para ello, Ir al Paso 3.
- **Paso 3** – Se debe completar el formulario de solicitud. En caso de usar Internet Explorer el formulario es el que se muestra en la figura 1a. En caso de usar Mozilla Firefox, el formulario se desglosa en dos pantallas , la primera solicita los datos personales y el nivel de seguridad de la clave (figura 1b) y la segunda pantalla, que se genera luego de hacer click en el botón “Solicitar Certificado”, solicita la elección del dispositivo criptográfico (figura 1c).

Figura 1a

Figura 1b

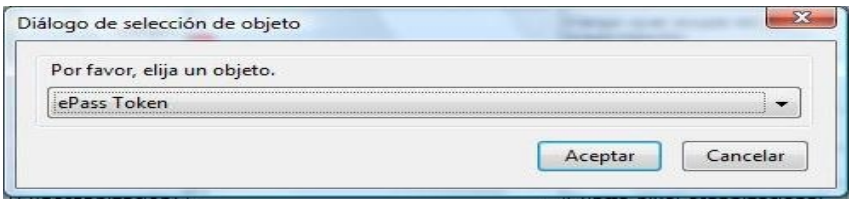


Figura 1c

Para completar los datos, utilizando cualquiera de los dos exploradores, en Organización colocar **Gobierno de la Provincia de Santa Fe**, en la primera sub-organización, indicar el ministerio o jurisdicción, en la siguiente la repartición y en la última Suborganización, colocar área u oficina, si corresponde..

A continuación, se debe elegir el proveedor de servicios criptográficos . Debido a que el certificado se almacenará en un token, se debe seleccionar el proveedor correspondiente como se muestra en las figuras 1a y 1c respectivamente. Por ejemplo, si el token que se está utilizando es el ePass2000, elegir “FTSafe ePass200 RSA Cryptographic Service Provider” en el caso de Internet Explorer o “ePass Token” en el caso de Mozilla Firefox, mientras que si el token es ikey2032 se debe elegir “Datakey RSA CSP” en Internet Explorer o el nombre asignado cuando se inicializó el token en el caso de Mozilla Firefox.

Por último, presionar Solicitar Certificado.

Una vez, ingresada la información anterior, de forma automática se presenta la pantalla correspondiente al Paso 4, donde se indican cuáles son las acciones siguientes. A continuación presionar en “Ir al Paso 5”.

Paso 5 – Se genera automáticamente la nota solicitando el certificado en la cual se indica un número de requerimiento, esta nota se debe imprimir porque es la documentación a presentar ante la Autoridad de Registro (AR) para el procedimiento de acreditación de identidad.

Paso 6 - Una vez impresa la nota, esperar la recepción del Mail de Verificación. En dicho correo electrónico, se solicita continuar con el procedimiento por lo que el usuario debe Ir al Paso 6b, enlace que se indica dentro del contenido del correo electrónico.

Paso 7 – Realizar el trámite de acreditación de identidad ante la Autoridad de Registro de manera personal y así, realizar la confirmación solicitada.

ANTE SU AUTORIDAD DE REGISTRO (AR)

Documentación a presentar:

- Documento Nacional de Identidad (D.N.I.)
- Fotocopia del D.N.I.
- Nota impresa con la firma hológrafa del solicitante, que certifica el requerimiento de solicitud de un certificado de clave pública.

En aquellos casos, en que la información del solicitante se encuentra fuera de la órbita de la Dirección Gral. de Recursos Humanos de la Provincia o en caso de ser personal contratado, además de la documentación anterior, el solicitante deberá presentar la Constancia de la Condición de Empleado de una Repartición (IFDFORM12), firmada por el Jefe del Area de Personal o Recursos Humanos o una autoridad superior.

EN SU COMPUTADORA LOCAL

Esperar la aprobación del certificado por parte de la Autoridad de Certificación, lo cual se notifica a través de un correo electrónico que le indicará que puede pasar a retirar su certificado de clave pública, en el sitio que se enlaza.

El retiro del certificado siempre se debe realizar en la misma computadora que se generó la solicitud y con el dispositivo criptográfico conectado para que el sistema deposite el certificado de clave pública en el mismo.

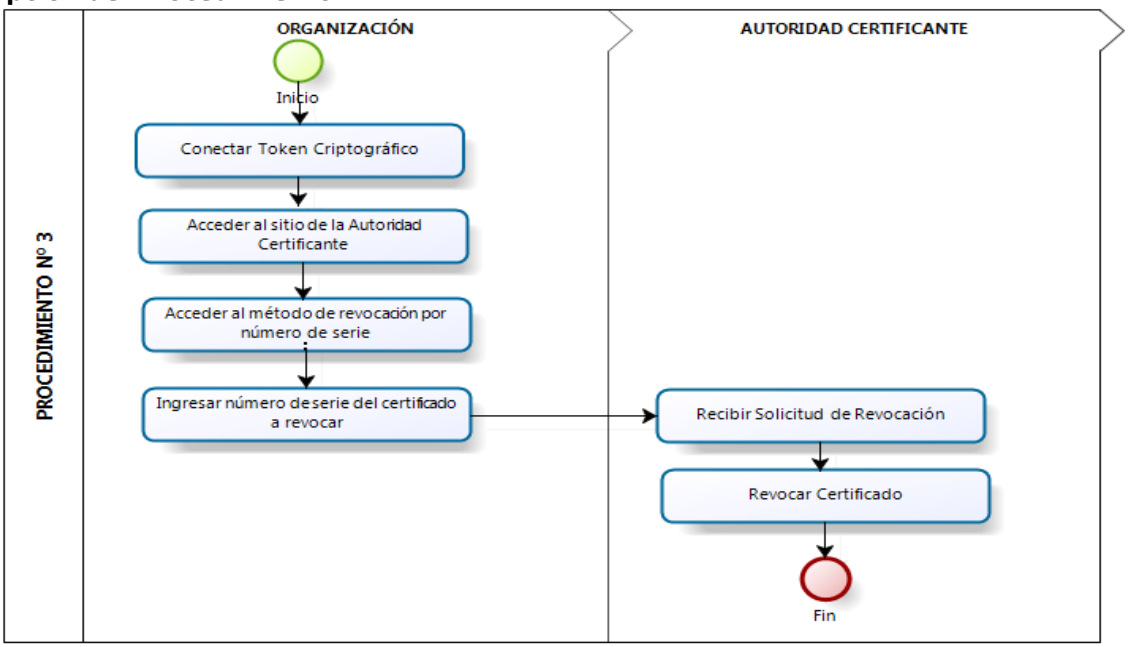
Procedimiento Nº 3 – Revocar un Certificado de Clave Pública

La revocación de un certificado digital se debe realizar toda vez que un suscriptor se encuentre en alguna de estas situaciones:

- Cuando se produzcan cambios en la información declarada al momento de su solicitud, tales como un cambio de función dentro de la repartición en la que trabaja, o cambio en la situación de revista, adscripción, traslado, ascenso, etc.
- Cuando exista algún tipo de riesgo o sospecha de que la clave privada asociada al certificado de clave pública se encuentre comprometida.
- En caso de pérdida o sustracción del dispositivo criptográfico que posee el certificado.
- Cuando cese su vínculo laboral con el organismo, dependencia o institución.
- Cuando el usuario decida inhabilitar el mismo para firmar digitalmente.

Es importante tener en claro que, una vez revocado el certificado digital, éste no deberá ser utilizado, aún cuando se encontrara en su período de validez. En caso de utilizar un certificado digital revocado para firmar digitalmente, esa firma no será válida.

Descripción del Procedimiento



EN SU COMPUTADORA LOCAL

Ingresar al sitio http://ca.pki.gov.ar. Se accede entonces al sitio de la Autoridad Certificante de la ONTI en el Gobierno Nacional y allí entrar ir al link “Revocar un Certificado Digital” . La primera página que presenta explica los pasos a seguir. Se debe presionar Ir al Paso 1. Se presentan entonces dos opciones, como se muestra en la Figura 2. Utilizar la Revocación por número de serie.

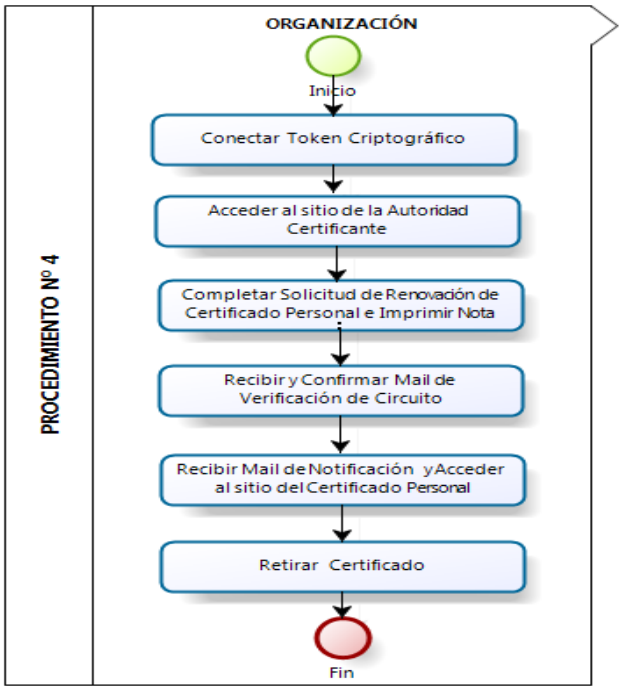
Figura 2

Una vez ingresado el número de serie en la pantalla mostrada anteriormente, se debe Enviar Solicitud a la Autoridad Certificante y esperar la notificación de que el certificado ha sido revocado. En caso de no conocer el número de serie del certificado, el mismo se puede buscar, ingresando al sitio http://ca.pki.gov.ar/search.html.

Procedimiento Nº 4 – Renovar un Certificado de Clave Pública

Todos los certificados otorgados por una Autoridad Certificante son emitidos, por cuestiones de seguridad, por un período de validez determinado, vencido este período el certificado no puede ser utilizado para firmar. Este procedimiento de renovación debe realizarse antes de la fecha de vencimiento del certificado y mientras el mismo no esté revocado, extendiendo de este modo el tiempo de vida útil del certificado de manera de poder continuar utilizándolo.

Descripción del Procedimiento



EN SU COMPUTADORA LOCAL

Ingresar al sitio http://ca.pki.gov.ar y seleccionar la opción Renovar un Certificado Digital. Se accede entonces al sitio de la Autoridad Certificante de la ONTI en el Gobierno Nacional. Debido a que el certificado está almacenado en un dispositivo criptográfico es necesario tener conectado el mismo antes de continuar.

El proceso va llevando al usuario a través de los siguientes pasos:

- Aceptar la Política de Certificación de la Autoridad Certificante
- Hacer la elección del método de renovación a utilizar. Allí se debe elegir la renovación automática.
- Hacer el pedido de renovación del certificado. Aquí se mostrará una ventana con los certificados almacenados y se debe seleccionar el que se quiera renovar.
- Recibir la confirmación de *Recepción de Solicitud de Renovación.*
- Imprimir la *Nota de Solicitud de Certificado de Clave Pública*. La impresión es para tener una constancia de la renovación, puede ser una impresión a documento pdf.
- Esperar la recepción del *Mail de Verificación* y realizar la confirmación solicitada en el mencionado correo electrónico.
- Esperar la recepción del *Mail de Notificación*, por parte de la Autoridad Certificante, el cual le indicará como acceder a su certificado para poder retirarlo.
- Acceder al sitio web de la Autoridad Certificante a fin de verificar la información contenida en el certificado a retirar.
- Retirar su certificado del sitio web de la Autoridad Certificante.

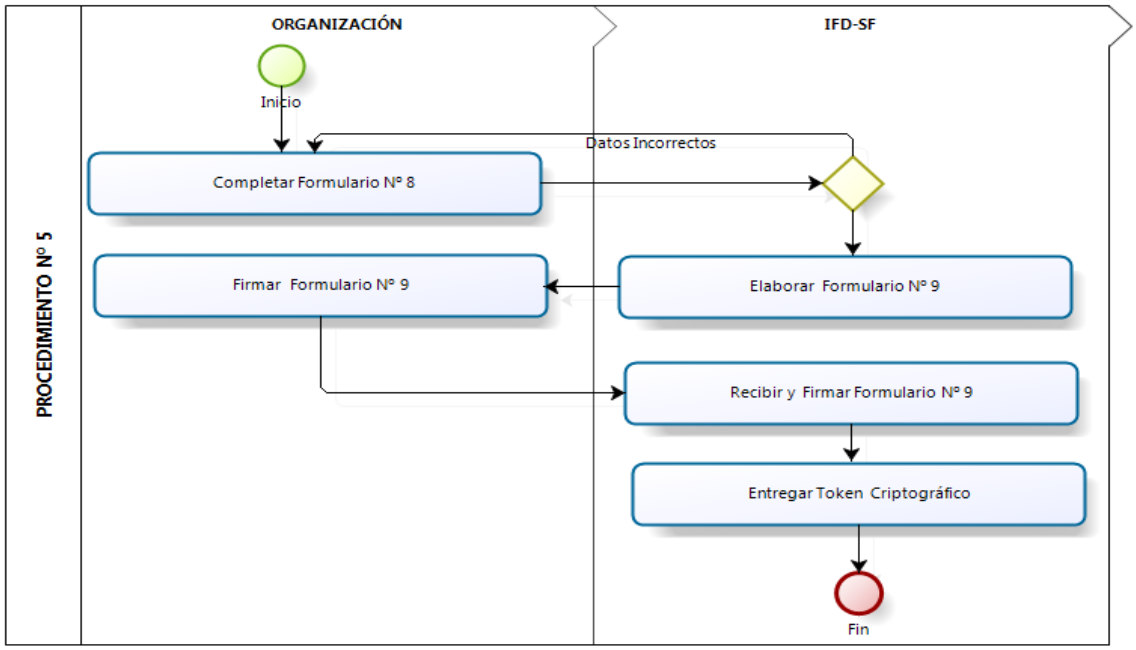
Procedimiento Nº 5 – Préstamo de Dispositivos Criptográficos

En virtud de que el máximo de seguridad para custodiar la clave privada lo proveen los dispositivos criptográficos que cumplan con la especificación indicada en la Recomendación Nº 1, se define que los organismos que implementen firma digital deberán prever la compra de los mismos para todas aquellas personas que van a utilizar certificados digitales.

En aquellos casos en los que el usuario requiere el uso inmediato de certificados digitales y no dispone aún del dispositivo criptográfico, la Infraestructura de Firma Digital le puede entregar uno en carácter de préstamo, para lo cual se deberá seguir el presente procedimiento.

La gestión de solicitud de préstamo de dispositivo y su correspondiente devolución, debe ser realizada por un informático de la jurisdicción, para todos los usuarios involucrados.

Descripción del Procedimiento



1. SOLICITAR DISPOSITIVO CRIPTOGRÁFICO

Los agentes designados para firmar digitalmente en un área o repartición, deberán ser informados a la IFD-SF e ingresados al sistema de Certificados, Agentes y Proyectos (SiCAP) que opera la Autoridad de Registro, según lo establecido en el Procedimiento Nº 1.

Estos agentes autorizados a firmar digitalmente, son los que deben disponer de un dispositivo criptográfico para almacenar su certificado digital. Cada área o repartición debe encargarse de la provisión de los mismos pero en caso de tener urgencia se puede solicitar un préstamo a la Infraestructura de Firma Digital, para lo cual, un informático de su jurisdicción deberá:

- Completar el Formulario Nº 8 del presente manual con los datos de la jurisdicción, proyecto, responsable informático que realiza la solicitud, cantidad de tokens que se piden y el detalle de las personas que lo utilizarán. Estas personas deben coincidir con las informadas para firmar digitalmente en el proyecto (Procedimiento Nº 1).
- El responsable de la solicitud, personal de la sectorial de informática, enviará dicho formulario por correo electrónico a la dirección firmadigital@santafe.gov.ar, indicando SOLICITUD DE DISPOSITIVO CRIPTOGRAFICO en el asunto del correo.
- La IFD-SF enviará un acuse de recibo del correo recibido y en el mismo, acuerda una fecha de

entrega y adjunta el Formulario Nº 9, que contiene el modelo de las actas compromiso. El informático imprimirá estas actas, para que complete y firme cada usuario a los que se les entregará un token.

2. RETIRAR DISPOSITIVO CRIPTOGRÁFICO

Para retirar el/los dispositivo/s criptográfico/s:

- El informático entrega las actas compromiso (Formulario Nº 9) correspondientes a cada uno de los usuarios para los que se solicitó el token. Estas actas deben estar firmadas por cada usuario ya que por la misma, se comprometen a conservar el dispositivo en perfectas condiciones y a restituir uno de iguales características y calidad o en su defecto, el otorgado en préstamo en caso de revocar o caducar su certificado digital. La devolución del dispositivo deberá realizarse dentro de los 90 días desde la fecha de firma del Acta Compromiso.
- La Infraestructura de Firma Digital entrega el dispositivo y completa la información en el Formulario Nº 10, indicando la fecha de entrega y los datos de la persona que retira.

3. USO DEL DISPOSITIVO CRIPTOGRÁFICO

Cuando el empleado ya cuenta con el dispositivo, el área informática correspondiente le deberá instalar el software para el manejo del mismo, el cual puede descargarse desde el portal de intranet en la dirección http://www.dpi.sfnet/firmadigital/drivers/. Se debe elegir el dispositivo, teniendo en cuenta la plataforma de sistema operativo de la máquina del usuario. Una vez instalado el driver, el dueño del token debe definir la contraseña de acceso y recordarla, porque el sistema la solicita toda vez que quiera firmar digitalmente.

4. DEVOLVER EL DISPOSITIVO CRIPTOGRÁFICO

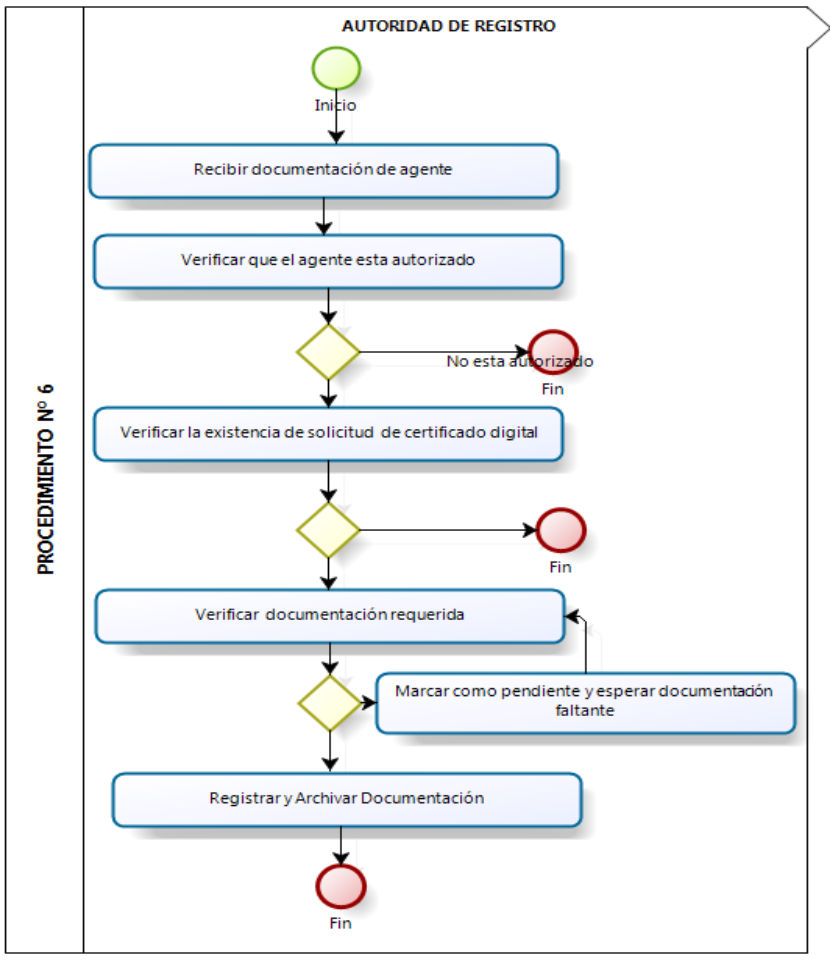
Cuando un usuario devuelve un dispositivo criptográfico, en la Infraestructura de Firma Digital se le entrega un recibo y se adjunta una copia del mismo al Acta de Compromiso firmada por el agente.

Luego, se registra la fecha de devolución en el Formulario 10, se formatea el dispositivo y se archiva en el almacenamiento físico destinado a tal fin.

Procedimiento Nº 6 – Gestión de Certificados de Clave Pública

El objetivo de este procedimiento es establecer una secuencia de pasos estándar que debe ejecutar el Oficial de Registro cada vez que se presenta un agente del Estado que ha solicitado un Certificado Digital a la Autoridad Certificante y debe autenticar su identidad.

Descripción del Procedimiento



1. RECIBIR DOCUMENTACION QUE PRESENTA EL SOLICITANTE

- Verificar que el solicitante se encuentra incluido en un proyecto aprobado por la Infraestructura de Firma Digital
- Controlar que el solicitante presenta toda la documentación requerida:
  - Documento Nacional de Identidad (D.N.I.)
  - Fotocopia del D.N.I.
  - Nota impresa que certifica el requerimiento
  - Constancia de la condición de empleado público (Formulario Nº 12) firmado por autoridad superior, en caso de que exista un Acta Compromiso del área de Recursos Humanos propia de la jurisdicción.
- Verificar la identidad del solicitante con el D.N.I. y que la fotocopia es copia fiel del original

2. VERIFICAR QUE EL AGENTE ESTA AUTORIZADO

Teniendo el CUIL del agente se debe consultar en el sistema SiCAP, que el agente ya este cargado y tenga algún proyecto asociado. Si no se encuentra el agente o no tiene proyectos asociados se debe indicar al agente que un informático de su jurisdicción se comunique con el área de Firma Digital.

3. VERIFICAR LA EXISTENCIA DE SOLICITUD DE CERTIFICADO DIGITAL

- Ingresar al sitio https://ca.pki.gov.ar/ccei/admin/.
- El sistema solicita un certificado digital para autenticar al Oficial de Registro. Una vez, seleccionado el certificado digital correspondiente, el sistema permite acceder al sistema de la Autoridad Certificante.
- Muestra los requerimientos pendientes. En esta pantalla, se puede seleccionar al solicitante o en su defecto, ingresar sus datos personales. Las opciones son:
  - Si el requerimiento no se encuentra en la lista de pendientes, se deberá solicitar al usuario que compruebe que su circuito de correo electrónico ha sido verificado y/o que realice nuevamente el trámite.
  - Si el requerimiento se encuentra como pendiente, ingresar a los datos del solicitante y:
    - Hacer firmar la fotocopia y nota de requerimiento al solicitante
    - Asignar Nº a la nota de requerimiento y firmar y sellar la nota
    - Emitir informe laboral

  Con esta información, las siguientes alternativas son las posibles:

  • Si todo está correcto, aprobar la emisión del certificado **(ESTADO DEL TRAMITE: APROBADO)**.

  • Si hay datos incorrectos en la solicitud, se deberá rechazar la solicitud en el sistema e informar al solicitante personalmente o por correo electrónico para que realice nuevamente el requerimiento **(ESTADO DEL TRAMITE: RECHAZADO).**

  • Si falta documentación, dejar el certificado como pendiente o rechazar.

  • Si hay datos dudosos, referidos a la situación de revista de la persona que no pueden validarse de forma inmediata, dejar el certificado como pendiente y luego, cuando se realice la validación total, enviar un correo electrónico al solicitante **(ESTADO DEL TRAMITE: EN PROCESO)**.

4. REGISTRAR Y ARCHIVAR DOCUMENTACION

- Una vez identificado el requerimiento en la lista de pendientes del sistema de la Autoridad Certificante, registrar la información en el sistema SiCAP, indicando lo siguiente:
  - Apellido y nombre
  - DNI
  - Nº de nota de requerimiento
  - Jurisdicción
  - Repartición
  - Cargo
  - Situación de revista
  - Teléfonos
  - Dirección de Correo Electrónico de Internet
  - Fecha de presentación
  - Estado del Trámite, los estados posibles son: APROBADO, RECHAZADO, EN PROCESO. Este último estado EN PROCESO, se refiere a la situación en la cual no se ha podido realizar la validación completa en el momento y en este caso, el Oficial de Registro deberá ponerse luego en contacto con la persona a través de correo electrónico informando el resultado de la verificación. En este caso, se deberá imprimir y archivar el correo electrónico que notifica esta situación al usuario.
  - Fecha de Aprobación en el sistema de la Autoridad Certificante
  - Fecha de Vencimiento del Certificado
- Una vez registrada la información en el SiCAP, se debe archivar lo siguiente:
  - Nota de requerimiento firmada por el solicitante

- Fotocopia del DNI firmada por el solicitante
- Informe del SARH / Acto administrativo que acredite la situación de revista firmado por el Oficial de Registro
- Correo electrónico notificando que su solicitud está en proceso, si corresponde.

5. CONTROLAR PERIODICAMENTE

- Diariamente, semanalmente o con la periodicidad que se determine según el volumen de certificados solicitados, se deberán realizar los siguientes controles:
- Consultar y/o imprimir los certificados de clave pública pendientes de aprobación que figuren en el sistema de la Autoridad Certificante
- Consultar y/o imprimir los certificados gestionados a través de la Autoridad de Registro para identificar si hay trámites con el estado EN PROCESO que se deban completar.
- A mediados de cada mes, consultar la información de los certificados digitales con estado APROBADO que tienen fecha de vencimiento dentro del próximo mes y notificar vía correo electrónico al agente para que inicie el proceso de renovación.

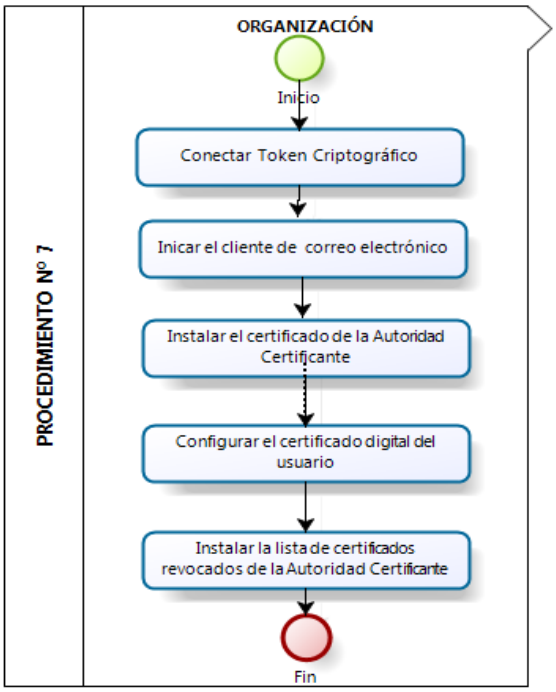
Procedimiento Nº 7 – Configuración de Cliente de Correo Electrónico

Este procedimiento es el que deberá seguir cualquier informático que necesite configurar un cliente de correo que envíe y/o reciba un correo electrónico firmado digitalmente.

Requerimientos

- Tener instalado el driver del dispositivo criptográfico en la computadora donde se va a utilizar el cliente de correo

Descripción del Procedimiento



1. CONFIGURAR EL CERTIFICADO DE LA AUTORIDAD CERTIFICANTE

- **MOZILLA THUNDERBIRD**
  Para el cliente de correo Mozilla Thunderbird, el procedimiento es el siguiente:

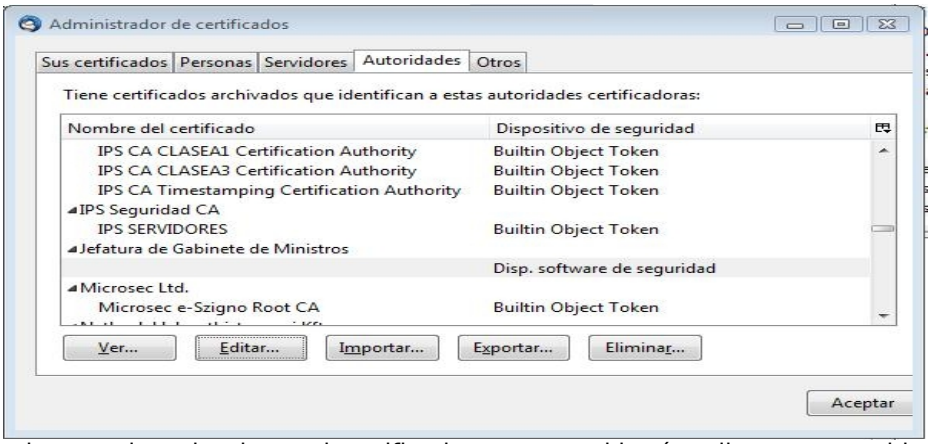
  Desde el navegador web Mozilla Firefox:

  - Acceder al menú “Herramientas”
  - En el menú herramientas elegir “Opciones”
  - En la ventana de Opciones elegir “Avanzado”, allí en la solapa “Cifrado” y luego presionar “Ver Certificados” y allí ir a la solapa Autoridades.
  - En la solapa de autoridades buscar la Autoridad Certicante de la ONTI que se identifica con el nombre "Jefatura de Gabinete de Ministros", una vez localizada la seleccionamos y apretar el boton "Exportar...". Allí pedira un nombre y directorio donde guardar el certificado.

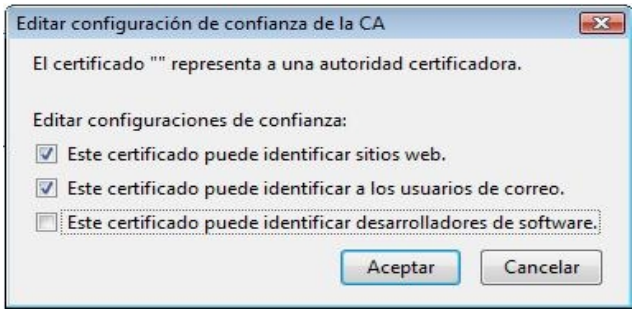
  Desde el cliente de correo Mozilla Thunderbird:

  - Acceder al menú “Herramientas”
  - En el menú herramientas elegir “Opciones”

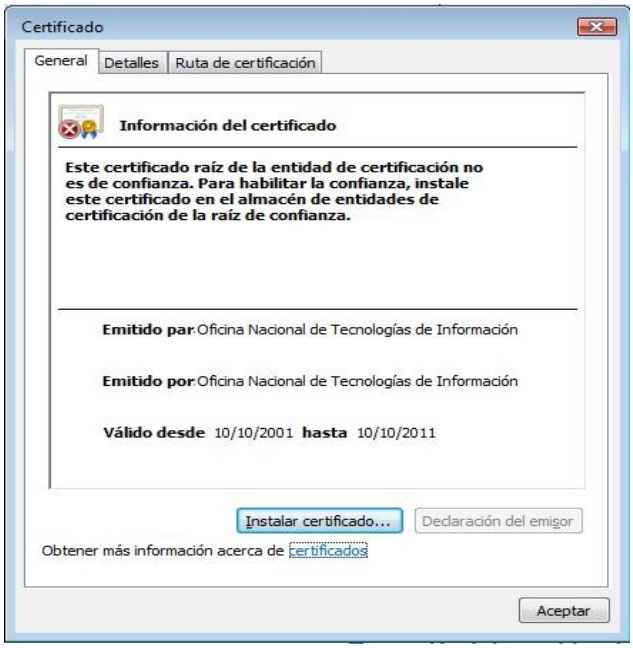
- En la ventana de Opciones elegir “Avanzado”, allí en la solapa “Cifrado” y luego presionar “Ver Certificados” y allí ir a la solapa Autoridades.
- En la solapa de autoridades apretar en boton "Importar..." y buscar el certificado de la Autoridad Certicante de la ONTI exportado previamente.



Una vez importado, seleccionar el certificado y apretar el botón editar para establecer las confianzas de dicho certificado. Elegimos las opciones de confiar para el sitio web y usuarios de correo electrónico.



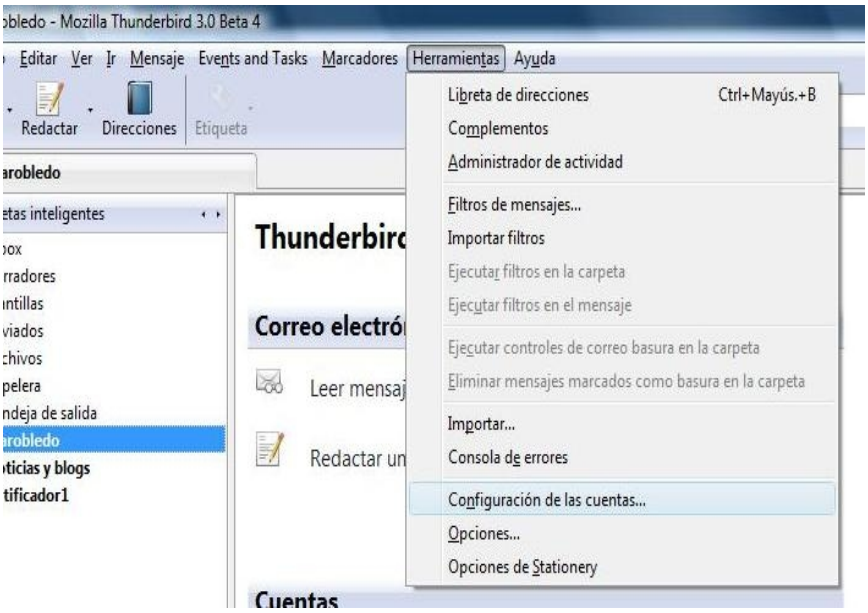
- **MICROSOFT OUTLOOK EXPRESS / MICROSOFT WINDOWS MAIL**
  Para los clientes de correo Microsoft Outlook y Microsoft Windows Mail los pasos son los siguientes:
- Desde el navegador web Internet Explorer, al sitio http://ca.pki.gov.ar/installCACert.html y apretar el botón "Instalar el certificado en su navegador".
- Aparecerá una ventana mostrando información del certificado, allí presionar "Instalar certificado...".



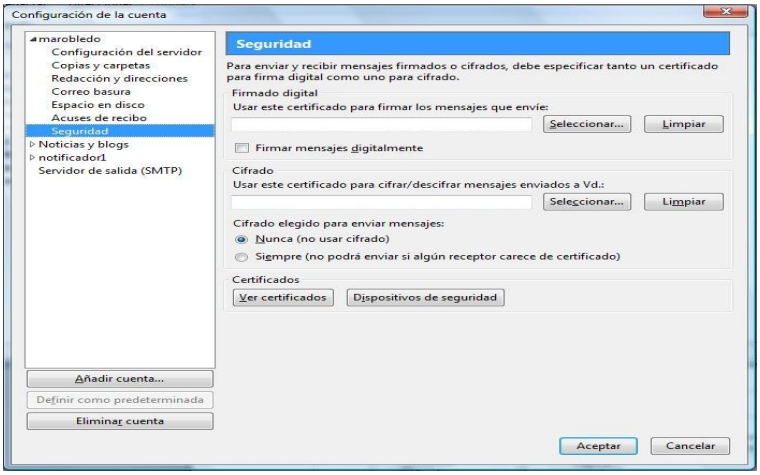
2. CONFIGURAR EL CERTIFICADO PERSONAL DEL USUARIO

- **MOZILLA THUNDERBIRD**

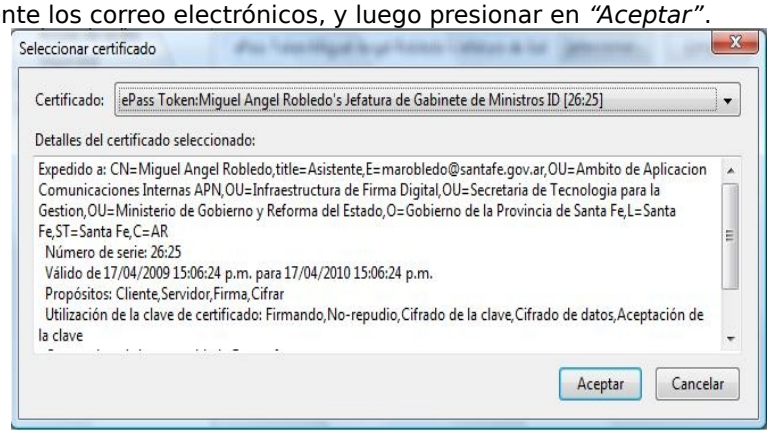
Seleccionar el menú “Herramientas” y elegir la opción *“Configuración de cuentas...”* de la lista.



A continuación aparecerá una ventana como la siguiente:



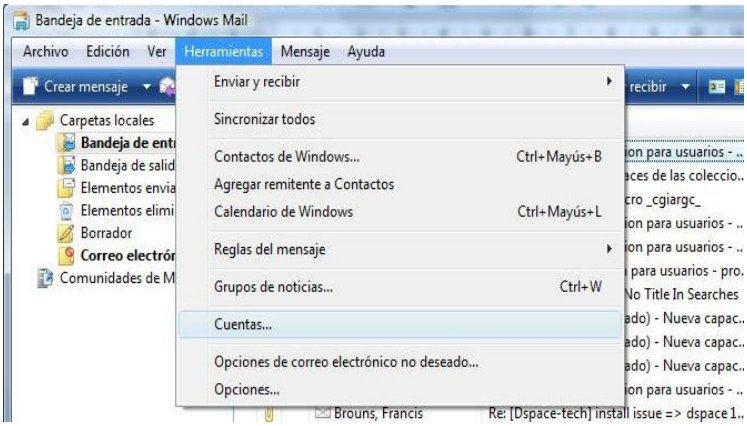
En el panel izquierdo de esta ventana, elegir la cuenta correspondiente y seleccionar "*Seguridad"*. En la parte derecha de la ventana, bajo la sección de Firma digital presionar en el botón *"Seleccionar..."*. Luego, aparecerá una ventana de donde se debe seleccionar de la lista el certificado que se desea utilizar para firmar digitalmente los correo electrónicos, y luego presionar en *"Aceptar"*.



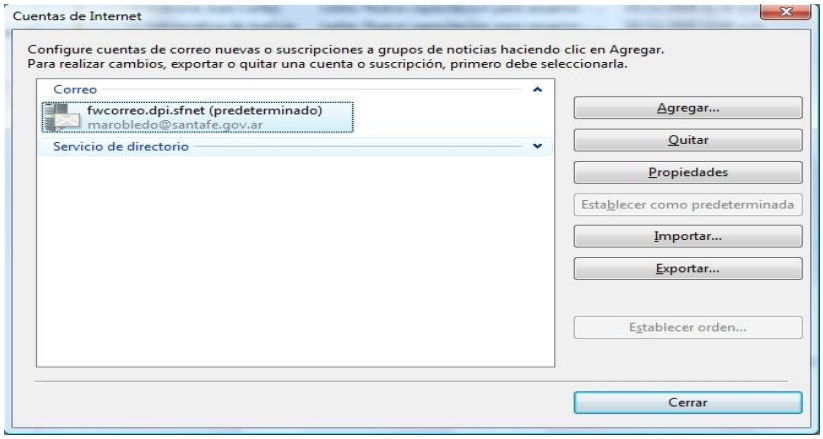
Los certificados que estén almacenados en el token empezarán con el nombre del dispositivo seguido por el nombre del certificado. Los certificados almacenados en la PC, no tendrán como prefijo ningún nombre.
Seleccionar el certificado que se encuentra almacenado en el Token. El programa preguntará si desea utilizar el mismo certificado para encriptar y desencriptar correo electrónicos. Presionar en "Aceptar" para finalizar el proceso. Luego, en la ventana de configuración de cuenta presionar "Aceptar" para confirmar sus preferencias.

- **MICROSOFT OUTLOOK EXPRESS / MICROSOFT WINDOWS MAIL**

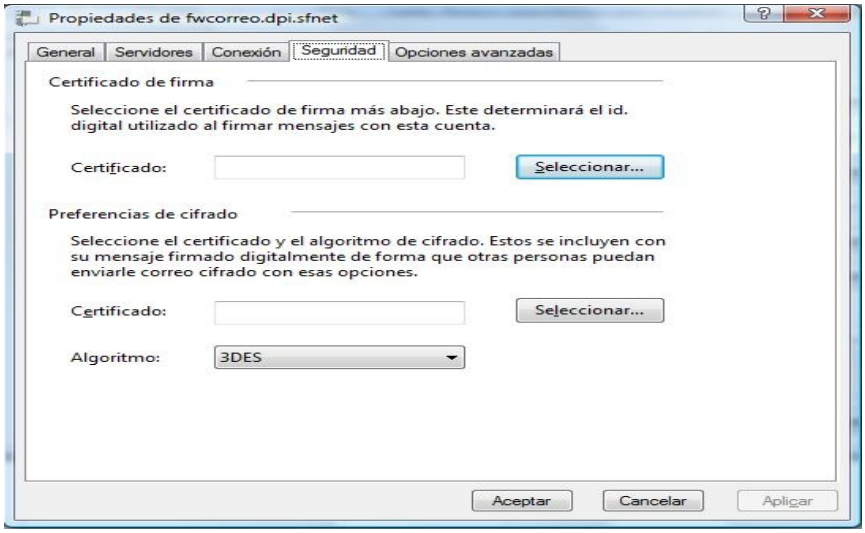
Seleccionar el menú "Herramientas" y elegir la opción "Cuentas." de la lista.



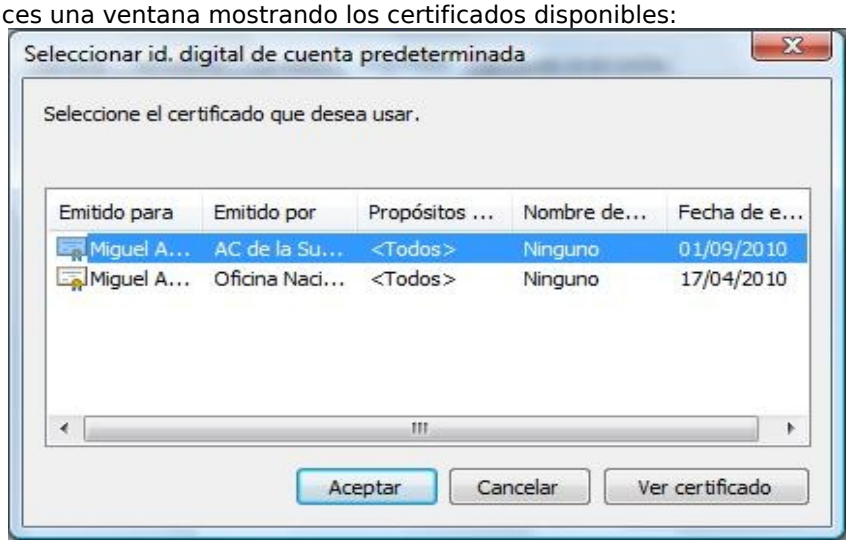
Se muestra una ventana con un listado de las cuentas configurados. Seleccionar la cuenta correspondiente y luego presionar “Propiedades”.



En la ventana de propiedades, presionar en la solapa “Seguridad”. Para elegir el certificado presionar en el botón “Seleccionar” en la sección de certificado de firma.



Aparece entonces una ventana mostrando los certificados disponibles:



Seleccionar el certificado que se desea y presionar “Aceptar” para cerrar esta ventana y confirmar las preferencias.

3. INSTALAR DE LA LISTA DE CERTIFICADOS REVOCADOS

Cuando una autoridad de certificación emite un certificado digital, este tiene un período máximo de validez, que en nuestro caso es de un año. El objetivo de este período de caducidad es obligar a la renovación del certificado para adaptarlo a los cambios tecnológicos.

En general, el certificado será renovado una vez transcurrido dicho período. Sin embargo, existen situaciones que pueden invalidar el certificado digital aún cuando éste no ha caducado, tales como:

- El usuario del certificado cree que su clave privada ha sido comprometida.
- Desaparece la condición por la que el certificado fue expedido. Por ejemplo, la persona se jubila, deja de participar en el proyecto al que esta asociado su certificado digital, cambia su situación de revista, etc.

- El certificado contiene información errónea o información que ha cambiado. Por ejemplo, una errata en los apellidos.

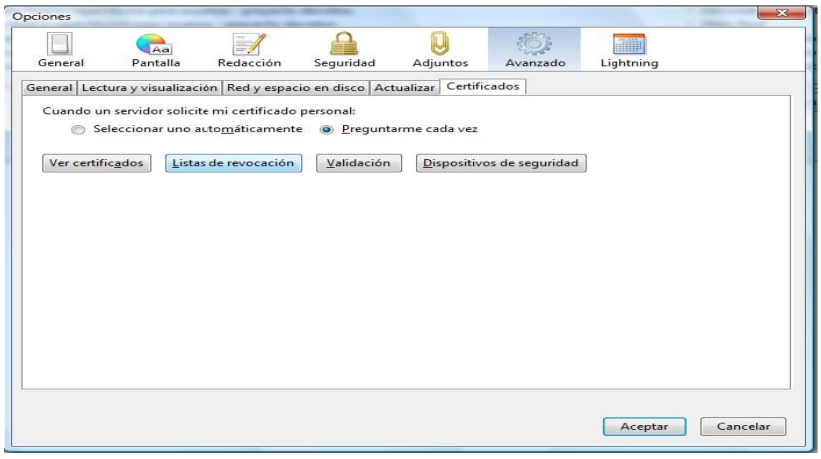
En estos casos, lo que se hace es revocar el certificado dejando sin validez al mismo a partir de ese momento. Para que el resto de los individuos que interactúan con dicho certificado sean notificados de dicha revocación, debe existir algún mecanismo para comprobar la validez de los certificados antes de su caducidad. Las CRLs (Certificate Revocation List) son uno de estos mecanismos.

Toda CRL, se identifica por una URL, que es el lugar donde se publica la misma. La CRL también está incluida en los certificados emitidos por la ONTI , por lo que de este modo, si las aplicaciones (clientes de correo, navegadores, etc.) utilizan esta información, pueden ser notificadas cuando un certificado está revocado. No todas las aplicaciones utilizan la CRL de forma automática, por lo que se debe configurar explícitamente esta funcionalidad.

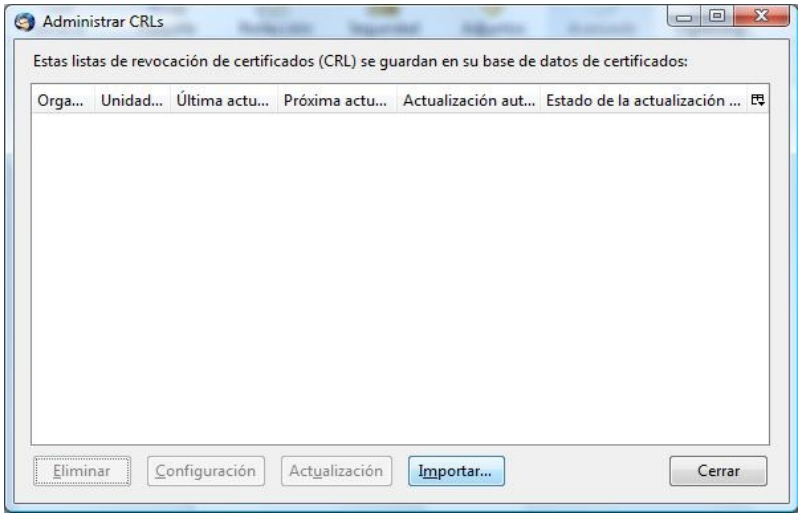
- **INSTALACION EN MOZILLA FIREFOX / MOZILLA THUNDERBIRD**

Tanto para el navegador web Mozilla Firefox como para el cliente de correo Mozilla Thunderbird, el procedimiento es el mismo. Los pasos son los siguientes:

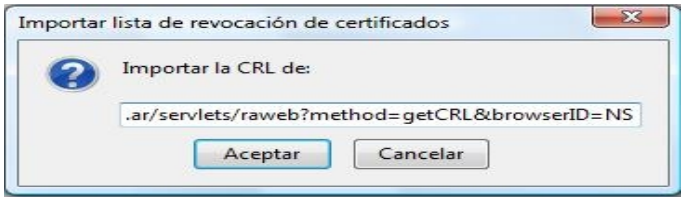
- Acceder al menú “Herramientas”
- En el menú herramientas elegir “Opciones”
- En la ventana de Opciones elegir “Avanzado”, allí en la solapa “Cifrado” y luego presionar “Lista de Certificados Revocados”



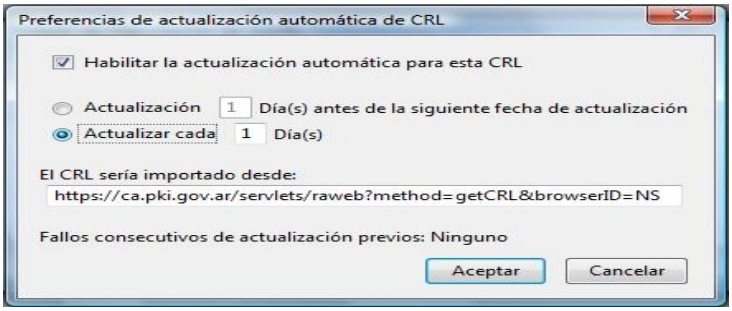
Aparecerá una nueva ventana donde se debe elegir “Importar”



Se presenta una nueva ventana donde se debe escribir la URL de la CRL a importar, que en nuestro caso es https://ca.pki.gov.ar/servlets/raweb?method=getCRL&browserID=NS



A continuación se nos informa que la importación se realizo con éxito y nos pregunta si se quiere activar la actualización automática, se elige que si y nos aparece la siguiente ventana, se presiona para que habilite las actualizaciones automáticas y que actualice cada un día.



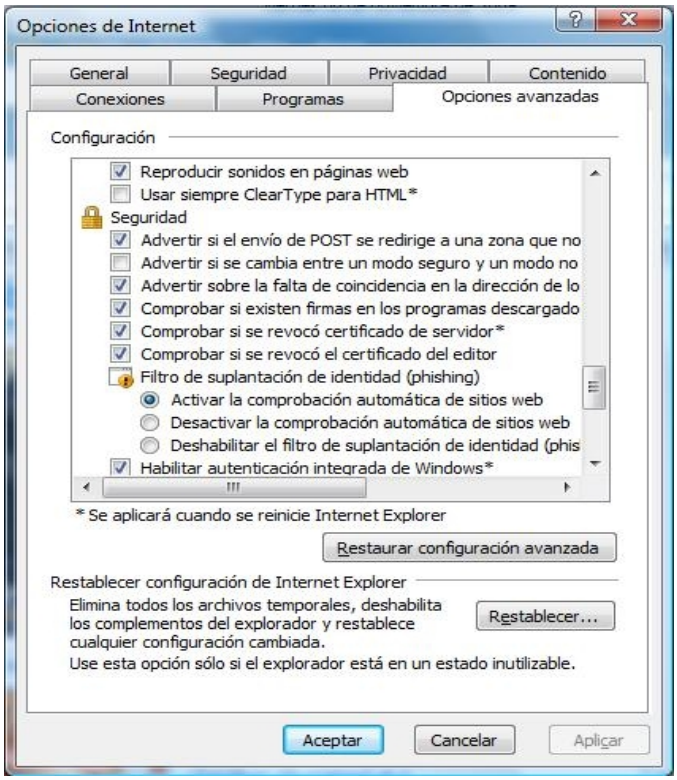
Por último, se debe seleccionar la CRL nuevamente y marcar la opción Actualizar.

- **INSTALACION EN MICROSOFT INTERNET EXPLORER / OUTLOOK EXPRESS / WINDOWS MAIL**

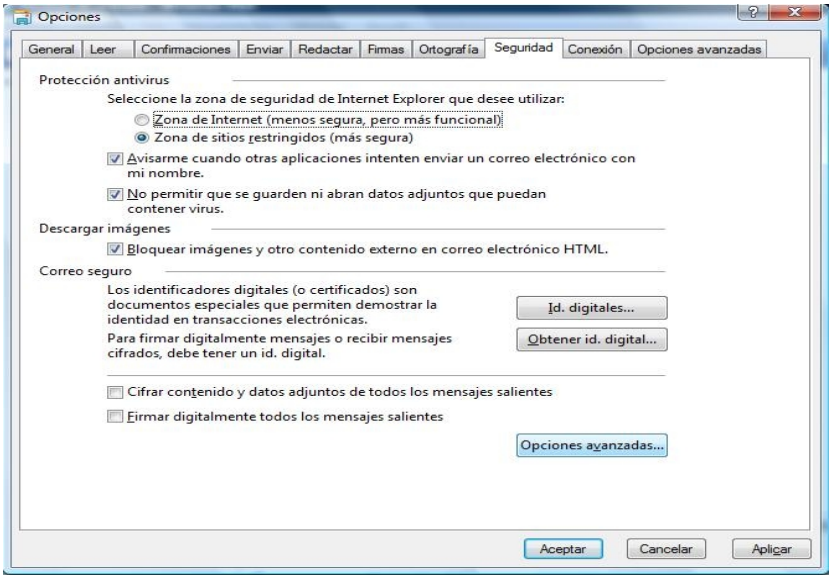
En el caso del navegador del navegador web y clientes de correo que provee Microsoft el procedimiento es el siguiente:

- Desde Internet Explorer acceder al menú “Herramientas”
- En el menú herramientas elegir “Opciones de Internet”

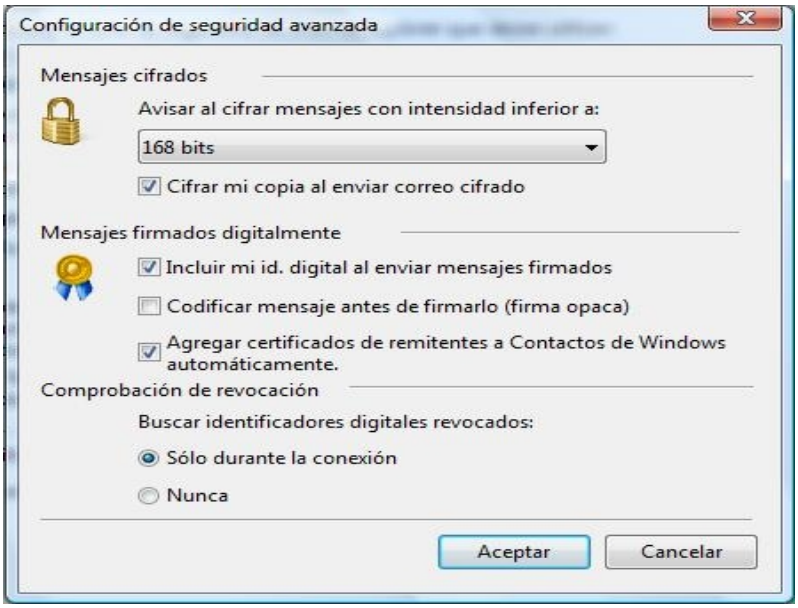
- En la ventana de Opciones elegir “Opciones avanzadas” y en las opciones de “Seguridad” elegir:
  Comprobar si se revocó certificado de servidor
  Comprobar si se revocó el certificado del editor



- Desde el cliente de correo, ya sea Outlook Express o Windows Mail, acceder al menú “Herramientas” y allí elegir la solapa “Seguridad” presionar en “Opciones avanzadas”



- En las opciones avanzadas, el la sección Chequeo de Revocaciones, marcar la opción “Sólo durante la conexión” como se muestra en la figura siguiente:



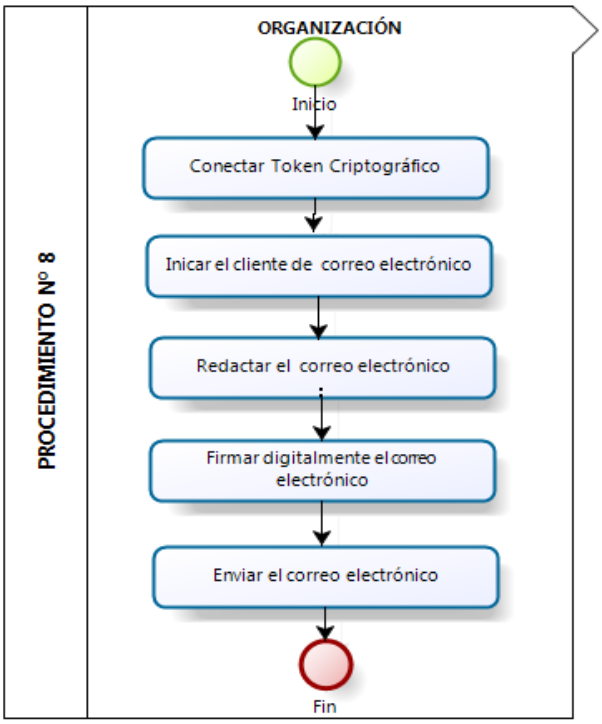
Procedimiento Nº 8 – Envío de Correos Electrónicos Firmados Digitalmente

Este procedimiento es el que deberá seguir cualquier usuario que envíe un correo electrónico firmado digitalmente.

Requerimientos

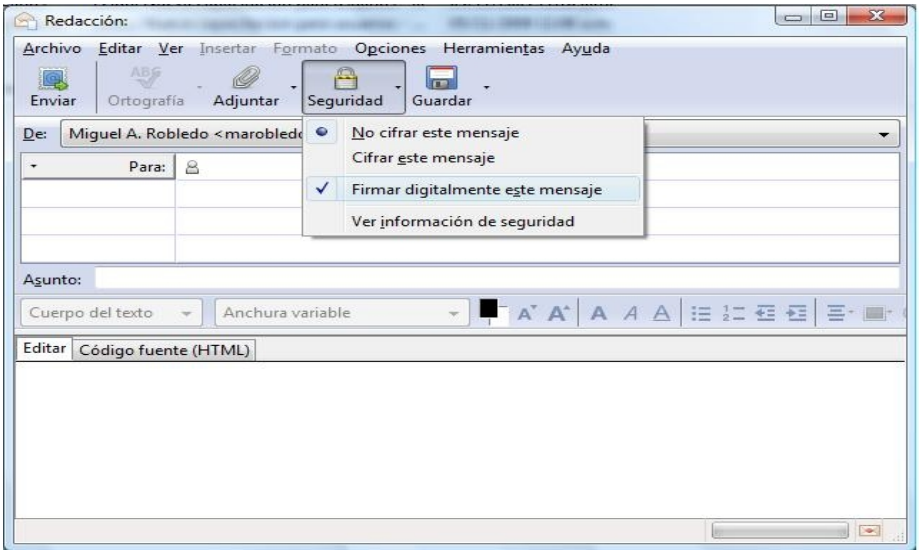
- Tener configurado el cliente de correo para operar con firma digital

Descripción del Procedimiento



- **MOZILLA THUNDERBIRD**

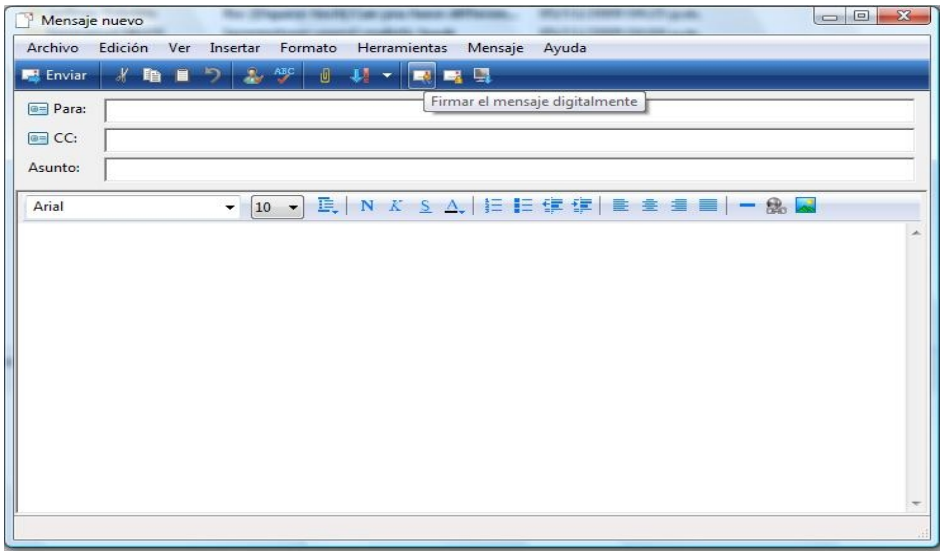
Presionar en el botón “Redactar”, completando todos los campos necesarios del nuevo mensaje y redactando el contenido del correo electrónico. Antes de enviar el correo, se debe firmar. Para ello, ir a la barra de herramientas y presionar en el botón “Seguridad”. Se desplegará un menú en el cual se debe seleccionar “Firmar digitalmente este mensaje”.



Una vez seleccionada esta opción enviar el correo electrónico presionando en el botón “Enviar”. El programa pedirá que se ingrese la clave del token. Si se ingresa correctamente la clave, el correo electrónico será firmado y enviado.

- **MICROSOFT OUTLOOK EXPRESS / MICROSOFT WINDOWS MAIL**

Presionar el botón “Crear Correo”, completar todos los campos necesarios del nuevo mensaje y redactar el contenido del correo electrónico. Antes de enviar, se debe firmar. Para ello, ir a la barra de herramientas y presionar en el botón de “Firma Digital”.



Presionar en “Enviar” para mandar el correo electrónico. El programa pedirá el ingreso de la clave del token. Si se lo ingresa correctamente, el correo electrónico será firmado y enviado.

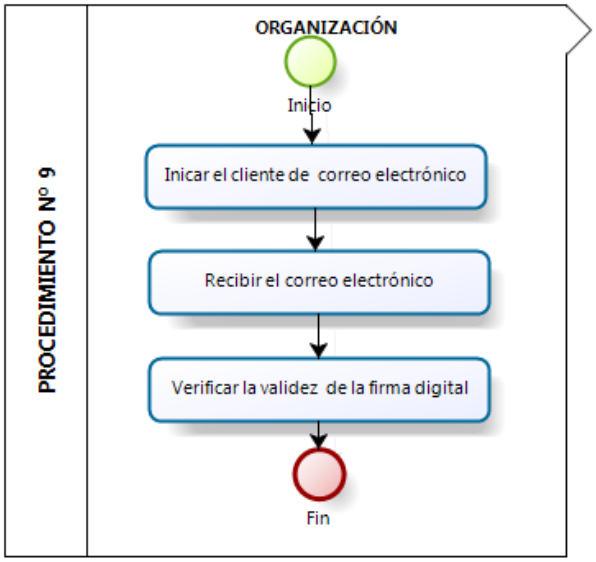
Procedimiento Nº 9 – Recepción de Correos Electrónicos Firmados Digitalmente

Este procedimiento es el que deberá seguir cualquier usuario que envíe y/o reciba un correo electrónico firmado digitalmente.

Requerimientos

- Tener configurado el cliente de correo para operar con firma digital

Descripción del Procedimiento



Al momento de recibir un correo electrónico firmado digitalmente, se debe verificar que el correo recibido y su firma sean válidos.

Si se recibe un correo electrónico cuya firma no pudo ser verificada, no necesariamente significa que el mismo haya sido modificado o enviado por otra persona. Muchas veces ocurre que el certificado con el cual se ha firmado, ha expirado o que simplemente la entidad que emitió el mismo, no está incluida entre sus entidades emisoras de confianza.

- **MOZILLA THUNDERBIRD**

En el caso de que llegue un correo electrónico firmado con un certificado en el cual se ha explicitado la confianza, al abrir el correo electrónico se ve un icono de correo electrónico firmado.

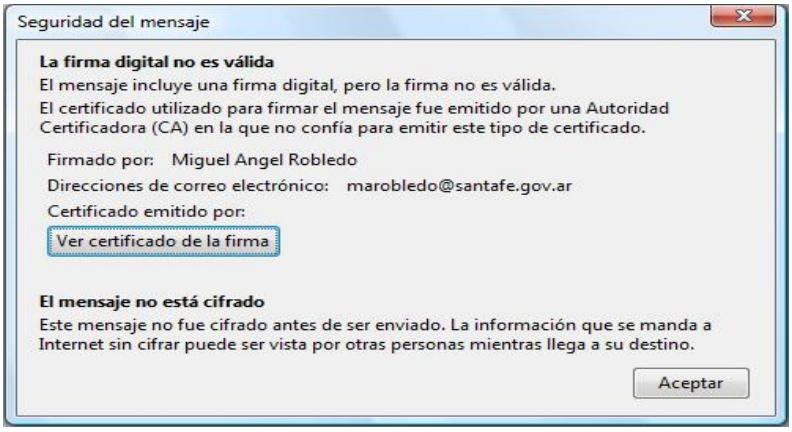
En el caso de que llegue un correo electrónico firmado con un certificado en el cual no se confía, al abrir el correo electrónico veremos un icono de advertencia .

En este caso, el símbolo de firma digital posee una cruz, lo que significa que la firma digital no se reconoce como válida por algún motivo. Estos motivos pueden ser diversos:

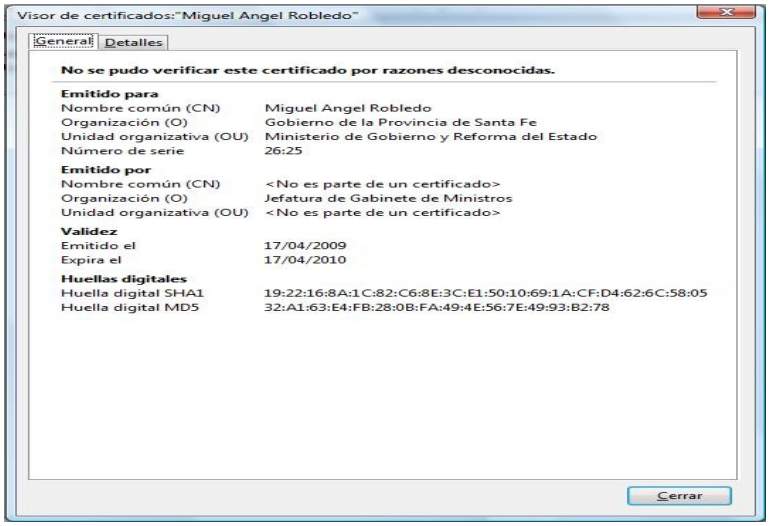
- que el certificado con el cual se firmó el correo haya expirado

- que el certificado haya sido revocado
- que no se confíe en la Entidad Certificante que emitió ese certificado

Si se presiona sobre ese icono, aparecerá una ventana como la que se muestra a continuación. La advertencia informa que la firma no es válida porque proviene de una Autoridad Certificante en la que no se confía.

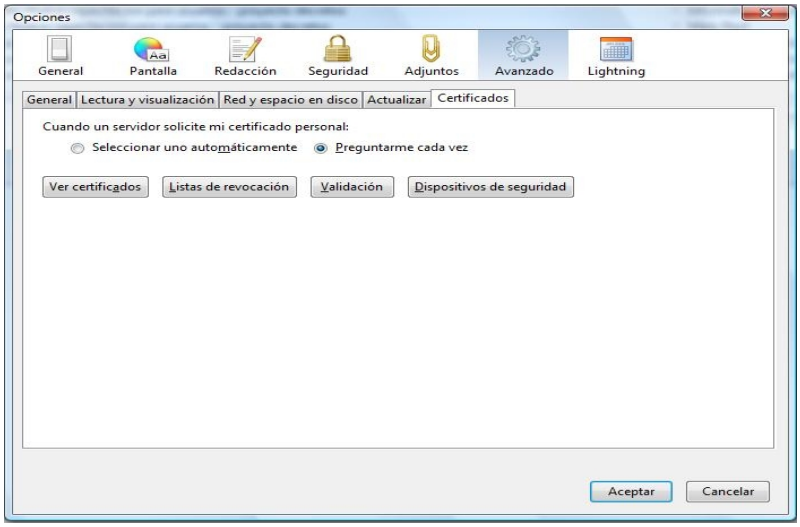


Si se presiona sobre “Ver certificado de firma” podrá ver una ventana que muestra todos los detalles del certificado.

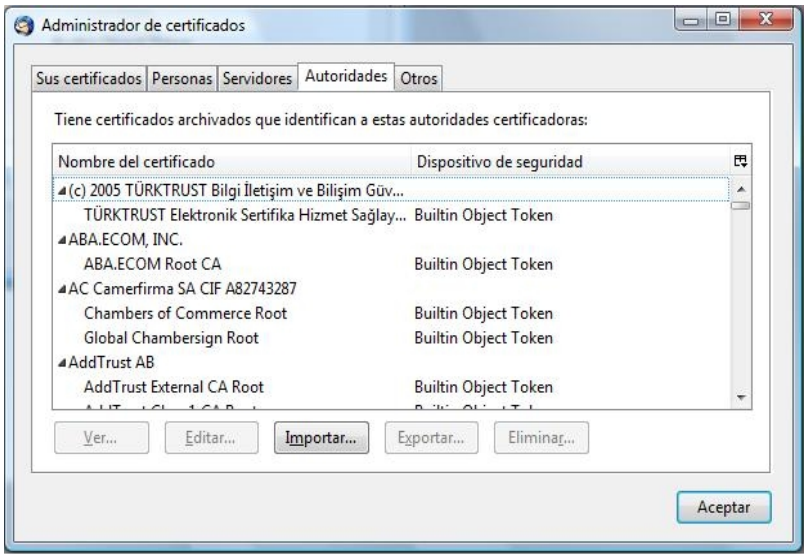


Para aceptar los certificados emitidos por una Autoridad Certificante (CA), se debe contar con el Certificado Raíz de dicha Autoridad Certificante instalado en el almacén de certificados del agente de correo electrónico. Para ello, se debe acceder al sitio de la CA (seguramente la misma estará disponible vía web para que cualquier usuario pueda descargar la clave pública de la CA) o pedirle a quien envió el correo electrónico firmado que lo proporcione.

Una vez que se tiene el certificado de la CA, ir al menú “Herramientas” y seleccione “Opciones”. En la parte superior de la ventana de opciones elegir la solapa “Avanzado” y allí “Ver certificados”.



Luego, en la nueva ventana de certificado ir a la solapa “Autoridades” y allí presionar en “Importar...” .



Buscar el certificado raíz de la Entidad Certificadora que se desea importar y aceptar la operación. Luego, aparecerá una ventana para seleccionar en qué casos se va a confiar en esta CA. Allí, tildar la opción de confianza para identificar usuarios de correo electrónico. Para terminar, presionar sobre “Aceptar”. Ahora, se puede ver que el icono del correo electrónico firmado ha cambiado por el de un certificado confiable.

- **MICROSOFT OUTLOOK EXPRESS / MICROSOFT WINDOWS MAIL**

En el caso de que llegue un correo electrónico firmado con un certificado en el cual se confía, al abrir el correo electrónico se ve en la parte superior derecha, un icono de correo electrónico firmado.

En caso contrario, o sea, si llega un correo electrónico firmado con un certificado en el cual no se

confía, al abrir el correo electrónico se ve en la parte superior derecha, un icono de advertencia, como el siguiente:

En este caso el símbolo de firma digital posee un un signo de error, lo que significa que la firma digital no se reconoce como válida por algún motivo. Estos motivos pueden ser diversos, tales como:

- Que el certificado con el cual se firmó el correo haya expirado
- Que el certificado haya sido revocado
- Que no se confíe en la Entidad Certificante que emitió ese certificado

Si se presiona sobre dicha imagen, la advertencia informa una serie de chequeos:

- Que el contenido NO ha sido modificado
- Que la firma NO es de confianza
- NO solicita confirmación
- Se ha chequeado la revocación del certificado

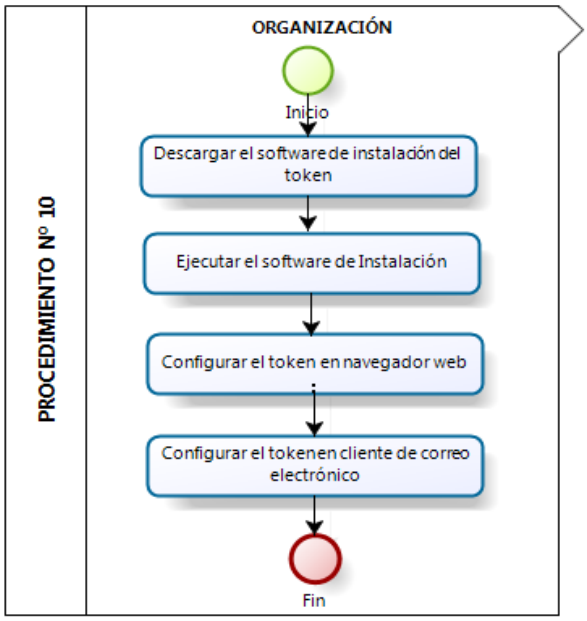
Si se presiona sobre “Ver certificados...” podrá ver una ventana que muestra todos los detalles del certificado.

Procedimiento Nº 10 - Guía de Instalación y Administración del Token ePass 2000

El token ePass2000 es utilizado actualmente en la Infraestructura de Firma Digital de Santa Fe . Este token cumple con lo especificado en la Recomendación Nº 1, brindando soporte para los sistemas operativos utilizados en nuestro ámbito: Microsoft Windows y GNU/Linux.

Para proceder con la instalación se debe estar seguro de no tener el token conectado a la PC.

Descripción del Procedimiento



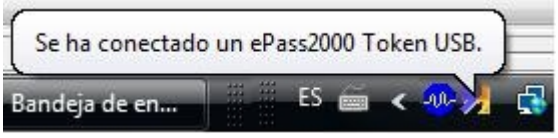
- **INSTALACION EN SISTEMAS WINDOWS**

En el caso de sistemas Windows, es necesario contar con permisos de administrador para poder instalar los drivers del token.

El primer paso es ejecutar el archivo “eps2k_stdSpanish.exe”provisto junto con el token. A continuación aparecerá un asistente que lo ayudará con la instalación del mismo, la cual consiste de una serie de pasos:

- La primera pantalla que aparecerá será una ventana de bienvenida.
- La segunda pantalla, pregunta por el soporte para VPNs (o sea, si el certificado para armar las VPNs está en el token) y la autenticación de inicio de windows por medio del token (logon) Deshabilitar esta opción dado que no se necesita.
- La tercera pantalla, nos indica el progreso de la instalación hasta que finaliza. Cuando finaliza se debe presionar en terminar.

Realizados los pasos anteriores, la primera primera vez que el usuario conecte el token, el sistema va a mostrar la lo siguiente en la barra de tarea:



Esto significa que la instalación del driver se ha realizado correctamente.

Para el caso en que se utilice Mozilla Firefox y Mozilla Thunderbird, es necesario cargar el módulo del

token. Para ello, hay que realizar los siguientes pasos en cada uno de ellos:

- Acceder al menú “Herramientas”
- En el menú herramientas elegir “Opciones”
- En la ventana de Opciones elegir “Avanzado”, allí la solapa “Cifrado” y luego presionar “Dispositivos de seguridad”
- Aparecerá una nueva ventana donde se debe elegir “Cargar”
- Aparecerá una nueva ventana con un campo para la elección del nombre con el cual se quiera identificar y un botón “Examinar” para buscar librería que provee el fabricante, la cual se encuentra en "c:\windows\system32\ep2pk11.dll"
- Una vez configurado, se acepta y se cierran las ventanas abiertas.

- **INSTALACION EN SISTEMAS GNU/LINUX**

Como requerimientos previos se necesita tener instalado:

- **libc6**: Incluye un conjunto de librerías estándares de GNU Linux. Se encarga de interpretar el lenguaje C y realizar la comunicación entre las aplicaciones desarrolladas en C y el kernel.
- **pcscd**: Middleware para acceder a una tarjeta inteligente con PC/SC. PC/SC (Personal Computer/Smart Card) es un conjunto de especificaciones para la integración de tarjetas inteligentes en computadoras personales. En particular se define un API de programación que permite a los desarrolladores trabajar de forma uniforme con lectores de tarjetas de distintos fabricantes (que cumplan con la especificación).

Habiendo instalado lo anterior, se puede proceder a la instalación del driver provisto junto con el token, realizando los siguientes pasos:

- Acceder a una consola con permisos de administrador
- Descomprimir el instalador con el siguiente comando: tar xvfz All-in-ONE-EnterSafe-ePass2000.tar.gz
- Ingresar al directorio generado: cd All-in-ONE-EnterSafe-ePass2000
- Ejecutar el instalador: ./install
- Reiniciar el demonio ngslodt para levantar el servicio middleware: /etc/init.d/ngslotd restart

Para el caso de Mozilla Firefox y Mozilla Thunderbird es necesario cargar el módulo del token poder empezar a utilizarlo. Para ello, hay que realizar los siguientes pasos en cada uno de ellos:

- Acceder al menú “Herramientas”
- En el menú herramientas elegir “Opciones”
- En la ventana de Opciones elegir “Avanzado” , allí la solapa “Cifrado” y luego presionar “Dispositivos de seguridad”
- Aparecerá una nueva ventana donde se debe elegir “Cargar”
- Aparecerá una nueva ventana con un campo para la elección del nombre con el cual se quiera identificar y un botón “Examinar” para buscar la librería que provee el fabricante, la cual se encuentra en "/usr/lib/libepsng_p11.so"
- Una vez configurado se acepta y se cierran las ventanas abiertas.

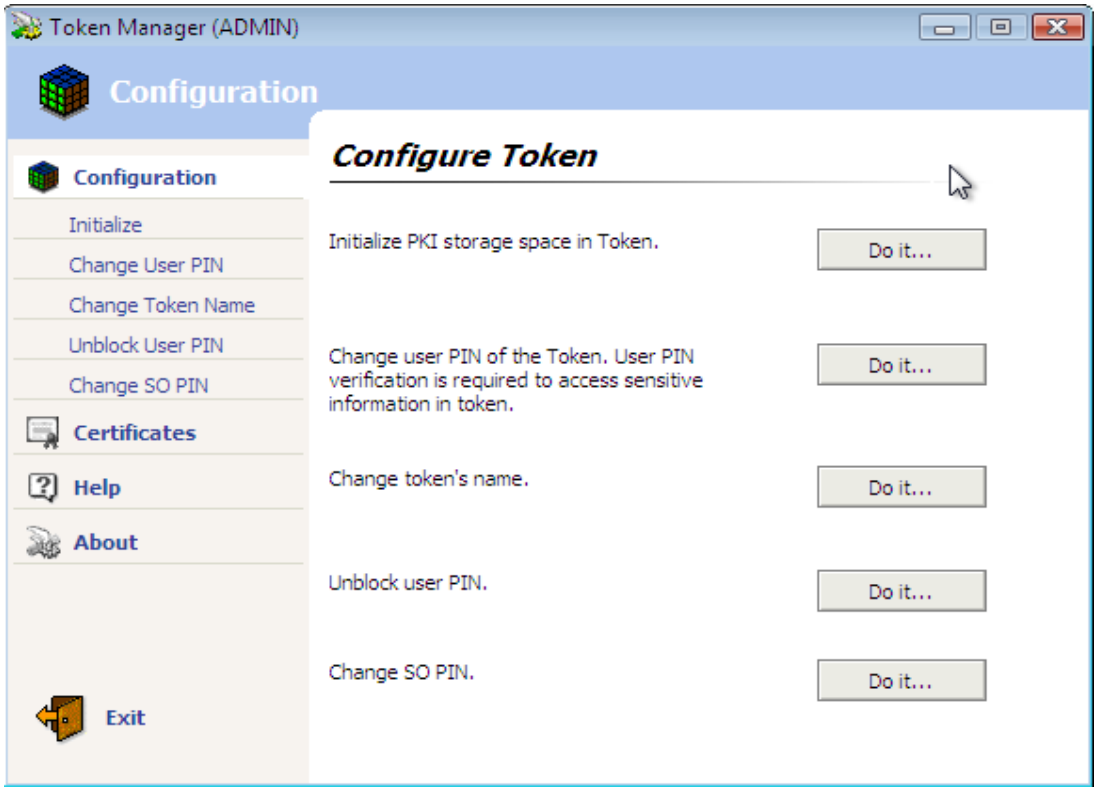
Software de Administración del token ePass 2000

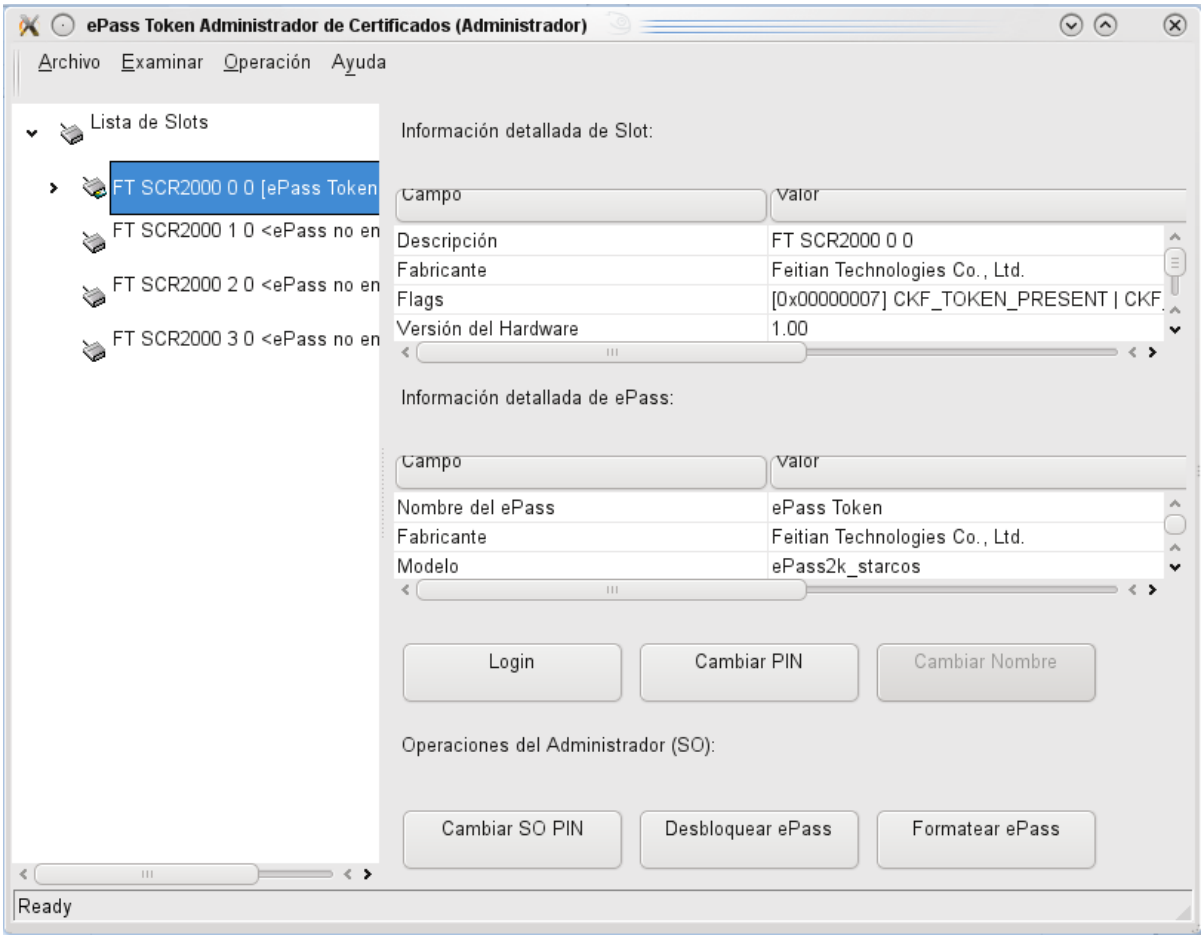
El token ePass 2000 cuenta con un software que permite realizar su administración. Por medio del mismo, un informáticos a cargo del mantenimiento del dispositivo, puede:

- **Agregar/Eliminar certificados del usuario al token:** Cabe destacar que cuando un certificado se elimina, es imposible volver a recuperarlo. Esto implica que es necesario revocar el certificado y gestionar uno nuevo, por lo que el borrado de un certificado es un tarea que se debe realizar con mucha conciencia.
- **Cambiar el PIN del usuario:** El PIN del usuario es la contraseña que se utiliza el usuario para acceder al token cada vez que se necesita firmar algún documento, cumple la misma función de controlar el acceso al dispositivo, por defecto viene con 12345678.
- **Cambiar el Nombre del token.**
- **Cambiar SO Pin:** El SO PIN es la contraseña que se utiliza el administrador para acceder al token cada vez que necesita realizar alguna tarea de mantenimiento.
- **Desbloquear ePass:** Tras varios intentos fallidos de ingresar la contraseña del token, el mismo quedará bloqueado por razones de seguridad, en éste caso el desbloqueo nos permite resetear el PIN del usuario.
- **Formatear ePass:** El formateo es útil cuando el token cambia de usuario y se lo quiere volver al estado inicial de configuración.

Para realizar estas funciones se debe ejecutar el archivo provisto junto con el token, *"epassMgr2K.exe"* en el caso de Windows o "*pkimanager_admin-1.0.100115.x86.tar.gz*" en el caso de Linux.

A continuación se muestran las pantallas del software de administración para plataforma Windows y Linux respectivamente.

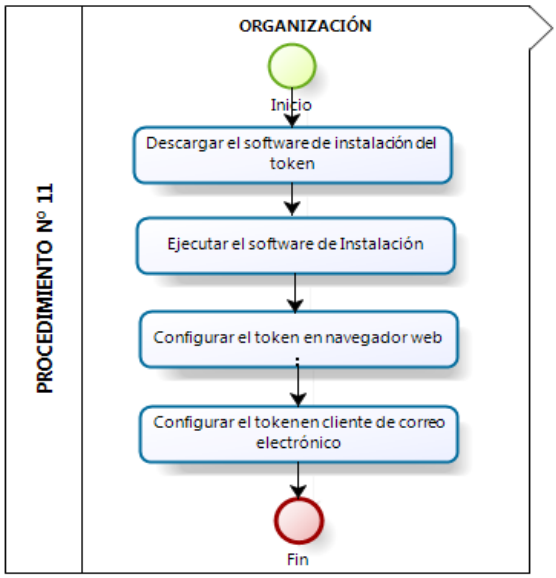



ePass Token Administrador de Certificados (Administrador)
Archivo Examinar Operación Ayuda
Lista de Slots
FT SCR2000 0 0 [ePass Token
FT SCR2000 1 0 <ePass no en
FT SCR2000 2 0 <ePass no en
FT SCR2000 3 0 <ePass no en
Información detallada de Slot:
Campo
Valor
Descripción
FT SCR2000 0 0
Fabricante
Feitian Technologies Co., Ltd.
Flags
[0x00000007] CKF_TOKEN_PRESENT | CKF
Versión del Hardware
1.00
Información detallada de ePass:
Campo
Valor
Nombre del ePass
ePass Token
Fabricante
Feitian Technologies Co., Ltd.
Modelo
ePass2k_starcos
Login
Cambiar PIN
Cambiar Nombre
Operaciones del Administrador (SO):
Cambiar SO PIN
Desbloquear ePass
Formatear ePass
Ready

Procedimiento Nº 11 - Guía de Instalación y Administración del Token ikey 2032

El token ikey2032 es utilizado actualmente en la Infraestructura de Firma Digital de Santa Fe . Este token cumple con lo especificado en la Recomendación Nº 1, brindando soporte para los sistemas operativos utilizados en nuestro ámbito: Microsoft Windows y GNU/Linux.

Descripción del Procedimiento



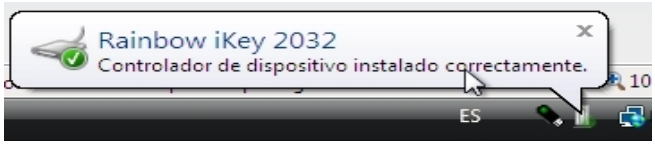
- **INSTALACION EN SISTEMAS WINDOWS**

En el caso de sistemas Windows, es necesario contar con permisos de administrador para poder instalar los drivers del token.

El primer paso es ejecutar el archivo “CSP.msi”provisto junto con el token. A continuación aparecerá un asistente que lo ayudará con la instalación del mismo, la cual consiste de una serie de pasos:

- La primera pantalla que aparecerá será una ventana de bienvenida, en la cual se debe presionar el botón *Next* para comenzar la instalación.
- La segunda pantalla, muestra una serie de datos sobre la instalación, debemos presionar el boton *Install* para continuar con la instalción.
- La tercera pantalla, nos indica el progreso de la instalación hasta que finaliza. Cuando finaliza se debe presionar el boton *Finish* terminar la instalación, el mismo pedirá reiniciar la pc.

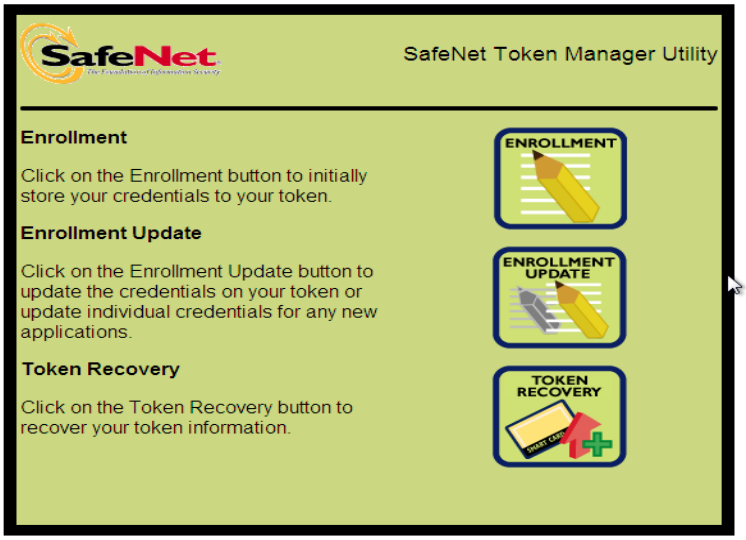
Realizados los pasos anteriores, la primera primera vez que el usuario conecte el token, el sistema va a mostrar la lo siguiente en la barra de tarea:



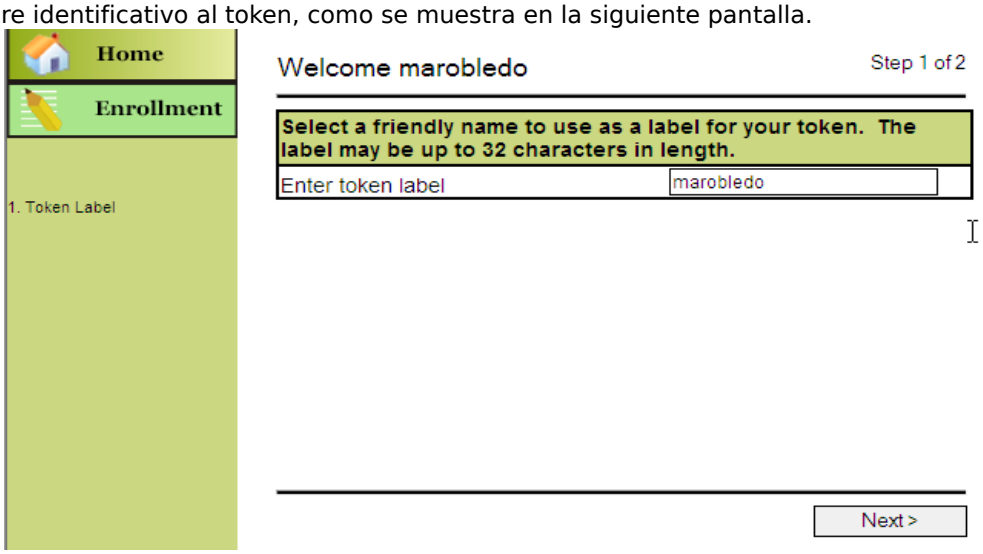
Esto significa que la instalación del driver se ha realizado correctamente.

Una vez instalado el token, si es la primera vez que se lo usa se debe realizar una configuración inicial del mismo. Para ello, hay que realizar los siguientes pasos en cada uno de ellos:

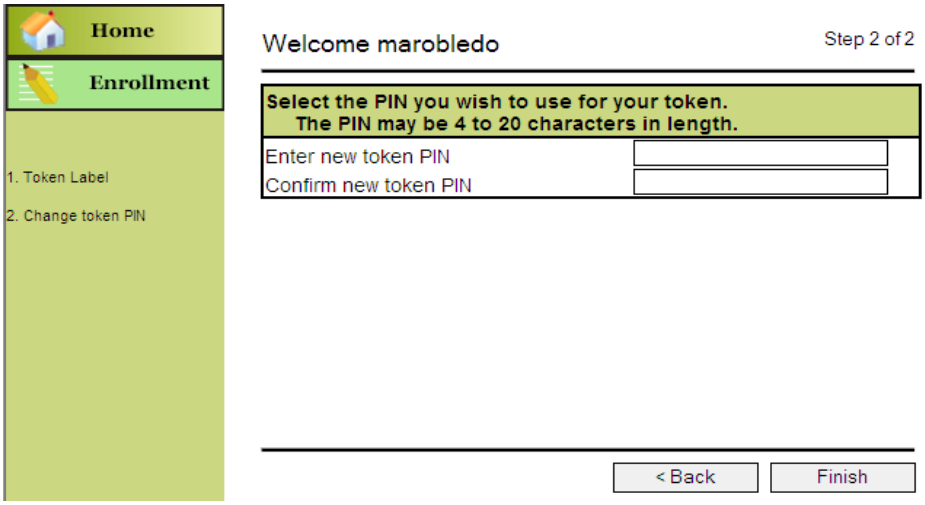
- Acceder al menú “Inicio” Windows.
- En el menú *Inicio* ingresar al submenu SafeNet → Borderless Security PK → SafeNet Token Manager Utility .
- Allí nos mostrará una página donde tenemos las opciones: Enrollment , Enrollment Update y Token Recovery. Allí elegimos la opción *Enrollment* (Registración).



- El proceso de registración (enrollment) consiste en dos pasos. El primero es la asignación de un nombre identificativo al token, como se muestra en la siguiente pantalla.



- Ingresado el nombre o etiqueta que lo identifique, se debe presionar el boton *Next* para acceder a la segunda pantalla, la cual consiste en la asignación de una contraseña inicial al token.



- Ingresada la contraseña y confirmada la misma, se debe presionar el botón *Finish* para terminar la registración del token.

Para el caso en que se utilice Mozilla Firefox y Mozilla Thunderbird, es necesario cargar el módulo del token. Para ello, hay que realizar los siguientes pasos en cada uno de ellos:

- Acceder al menú “Herramientas”
- En el menú herramientas elegir “Opciones”
- En la ventana de Opciones elegir “Avanzado”, allí la solapa “Cifrado” y luego presionar “Dispositivos de seguridad”
- Aparecerá una nueva ventana donde se debe elegir “Cargar”
- Aparecerá una nueva ventana con un campo para la elección del nombre con el cual se quiera identificar y un botón “Examinar” para buscar librería que provee el fabricante, la cual se encuentra en "c:\windows\system32\dkck201.dll"
- Una vez configurado, se acepta y se cierran las ventanas abiertas.

- **INSTALACION EN SISTEMAS GNU/LINUX**

Como requerimientos previos se necesita tener instalado:

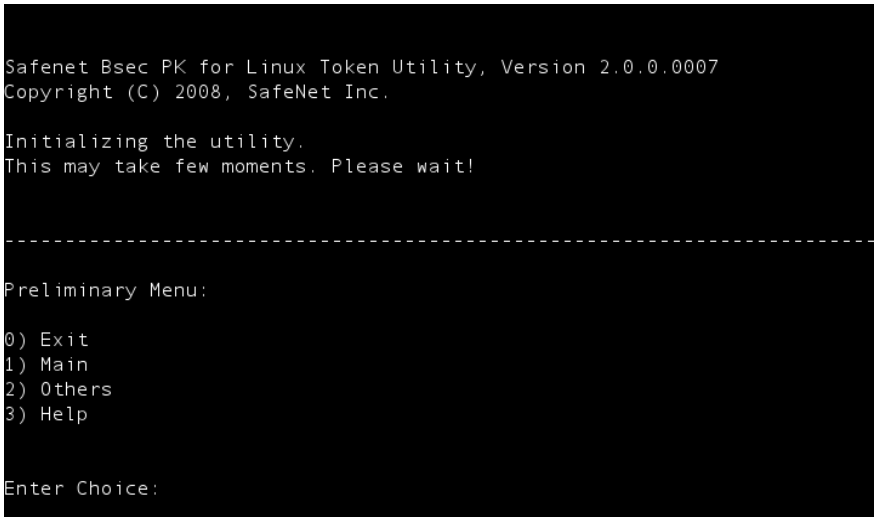
- **libc6**: Incluye un conjunto de librerías estándares de GNU Linux. Se encarga de interpretar el lenguaje C y realizar la comunicación entre las aplicaciones desarrolladas en C y el kernel.
- **pcscd**: Middleware para acceder a una tarjeta inteligente con PC/SC. PC/SC (Personal Computer/Smart Card) es un conjunto de especificaciones para la integración de tarjetas inteligentes en computadoras personales. En particular se define un API de programación que permite a los desarrolladores trabajar de forma uniforme con lectores de tarjetas de distintos fabricantes (que cumplan con la especificación).
- **gcc:** Compilador para C, C++, Objective C y Fortran. Es capaz de recibir un programa fuente en cualquiera de estos lenguajes y generar un programa ejecutable binario.
- **make:** Herramienta para creación de ejecutables, o programas, para su instalación, la limpieza de los archivos temporales en la creación del fichero, etc.

Habiendo instalado lo anterior, se puede proceder a la instalación del driver provisto junto con el token, realizando los siguientes pasos:

- Acceder a una consola con permisos de administrador

- Descomprimir el instalador con el siguiente comando: unzip BSecPKLinux-2.0.0.0007.zip
- Ingresar al directorio generado: cd BSecPKLinux-2.0.0.0007/
- Ejecutar el instalador: sh install-BSecPK-v2.0.0.sh . Realizará una serie de preguntas durante la instalación, se debe responder a todo con " y " , controlar que no halla errores durante la instalación. En caso de haber error seguramente sea por falta de alguna dependencia, se debe instalar el requerimiento y ejecutar el instalador nuevamente hasta que concluya sastifactoriamente.

- Una vez terminada la instalación del token se debe actualizar la librería de acceso al mismo debido a que la original tiene conflictos. Para ello se debe copiar la librería libsfntpkcs11.so.2.0.0.7 que se entrega junto con el instalador en el directorio /usr/local/SafeNet/lib/ : cp libsfntpkcs11.so.2.0.0.7 /usr/local/SafeNet/lib/
- Luego, se debe reconfigurar la librería: ldconfig /usr/local/SafeNet/lib/
- Una vez terminada la instalación se debe ejecutar el software administración, para comprobar que todo funciona correctamente, mediante el comando: TokenUtility



- Una vez finalizada la instalación del token, si es la primera vez que se lo utiliza se debe realizar la configuración inicial mediante el comando TokenUtility. Allí se deben realizar los siguientes pasos:

1. Ingresado al menú de TokenUtility, elegir la opción 1) Main .
2. Dentro del menú *Main* elegir la opción 1) Token .
3. Dentro del menú *Token* elegir la opción 1) Setup .
4. Dentro del menú *Setup* elegir la opción 1) Initialize Token, allí hace una descripción de los objetivos y pregunta si se desea continuar, se debe responder "Y" .
5. Luego del paso anterior el token queda inicializado con una contraseña por defecto (Password#1) y un nombre aleatorio en base al número de serie. Estos parámetros pueden, luego, ser cambiados desde TokenUtility → 1) Main → 1) Token → 4) Change Token Parameters.

Para el caso de Mozilla Firefox y Mozilla Thunderbird es necesario cargar el módulo del token poder empezar a utilizarlo. Para ello, hay que realizar los siguientes pasos en cada uno de ellos:

- Acceder al menú “Herramientas”
- En el menú herramientas elegir “Opciones”
- En la ventana de Opciones elegir “Avanzado” , allí la solapa “Cifrado” y luego presionar “Dispositivos de seguridad”
- Aparecerá una nueva ventana donde se debe elegir “Cargar”
- Aparecerá una nueva ventana con un campo para la elección del nombre con el cual se quiera identificar y un botón “Examinar” para buscar la librería que provee el fabricante, la cual se encuentra en "/usr/local/Safenet/lib/libsfntpkcs11.so"
- Una vez configurado se acepta y se cierran las ventanas abiertas.

RECOMENDACIONES

Recomendación Nº 1 – Especificación Mínima para Dispositivo Criptográfico (Token)

Presentación:

- Carcasa de protección compuesta de un material robusto, resistente al agua y firmemente sellado a fin de no permitir el ingreso de líquidos.
- Características de 'tamper-evident'.
- Interfase estándar USB tipo A.
- Debe tener un LED indicador de actividad.

Características Técnicas:

- Tecnología Plug-and-Play para facilitar su utilización con aplicaciones cliente.
- Debe contar con certificación FIPS 140, por lo menos con overall level 2.
- Debe permitir implementar 'Doble Factor' de autenticación, es decir que es necesario a tal fin poseer la llave criptográfica y una contraseña, o rasgo verificable por algún procedimiento biométrico (por ejemplo la huella dactilar).
- Conectividad a través de los estándares Crypto API y PKCS#11 .

Especificaciones Técnicas:

- Plataformas soportadas:
  - Windows XP/Vista.
  - GNU/Linux.
- APIs y estándares soportados:
  - PKCS#11 v2.01 o superior,
  - Microsoft Crypto API (CAPI) 2.0 o superior,
  - PC/SC (Personal Computer Smart Card),
  - X.509 v3,
  - SSL v3,
  - IPSec/IKE
  - OpenSSL (opcional)
  - Tamaño de memoria de al menos 32 Kbytes.
  - Algoritmos de seguridad incorporados:
  - Encriptación con claves asimétricas: RSA 2048-bits o superior.
  - Firma Digital: RSA 2048-bits o superior.
  - Generación de claves simétricas: DES, 3DES (Triple DES).
  - Algoritmo de Hash: SHA-1.
  - Algoritmo de Generación Aleatoria de Números (RNG) (La generación aleatoria de números debe realizarse por hardware e internamente en la llave criptográfica).
  - Los dispositivos deberán contar con sus respectivas licencias de uso (de corresponder) y los correspondientes drivers y aplicativos necesarios para su funcionamiento.
  - El oferente deberá garantizar soporte técnico, así como también soporte de actualización de los drivers y firmware del dispositivo, sin costo alguno para el organismo, durante un período no inferior a 2 años a partir de la fecha de compra del mismo.
  - El oferente deberá entregar el software, los manuales y demás documentación preferentemente en idioma español, o en su defecto, en idioma inglés.

Aplicaciones Soportadas:

- Clientes de e-mail y navegadores web:
  - Microsoft Outlook / Outlook Express & Internet Explorer
  - Mozilla Firefox & Mozilla Thunderbird.
- Windows logon (opcional).

Recomendación Nº 2 - Configuración Mínima de Equipo para Operar con Firma Digital

Una estación de trabajo que participe en un proyecto de firma digital. debería tener como mínimo los siguientes componentes:

- **Plataforma de hardware recomendada**
  - Microprocesador: 1 GHz o superior.
  - Memoria RAM: 512 MB o superior.
  - Al menos 1 puerto USB libre.

- **Software:**
  - Sistema Operativo GNU/Linux o Microsoft Windows XP Service Pack 2.
  - Máquina virtual de Java versión 1.6.5 o superior
  - Java JCE.
  - OpenOffice 2.4 o superior
  - Adobe Reader 7.0 o superior
  - Navegador Web Mozilla Firefox 2.0 o superior
  - Navegador Web Internet Explorer 6.0 o superior
  - Agentes de Correo Mozilla Thunderbird 2.0 o superior
  - Outlook Express 5.0 o superior
  - Software para firmado de Archivos SiFEP .
  - Software utilizado para acceder al token (middleware y software de administración del dispositivo)

Las características detallas son las necesarias para operar con firma digital, y podrían no incluir la totalidad de los componentes que se pueden encontrar en una estación de trabajo tipo.

Las versiones del software citadas son las mínimas requeridas, se recomienda siempre tener la última versión estable por cuestiones referentes a sus actualizaciones referentes a seguridad y estándares.

Recomendación Nº 3 - Aspectos de Seguridad Mínimos del Equipo de Trabajo

Es conveniente que la computadora personal que se utilice para firmar digitalmente, cuente con algunas medidas mínimas de seguridad. Por ello, se recomiendan a continuación aspectos que deberán tenerse en cuenta, en el nivel del entorno, del hardware y del software, para que su estado sea confiable.

Se sugiere que los aspectos que se detallan a continuación se evalúen y acuerden entre el usuario y el responsable informático de su jurisdicción.

- **DEL ENTORNO DE TRABAJO**

Esta sección comprende mecanismos, generalmente de prevención y detección, destinados a proteger físicamente cualquier recurso del sistema. En general, los problemas que se pueden tener en un recurso informático pueden provenir de alguna de las siguientes razones:

* Acceso físico
* Desastres naturales
* Alteraciones del entorno

Acceso físico: Si alguien que desee atacar un sistema tiene acceso físico al mismo, todo el resto de medidas de seguridad implantadas se vuelven muy débiles. Por ello, siempre es necesario controlar el acceso a las oficinas y en particular no dejar expuesto el dispositivo de almacenamiento de claves.
Desastres naturales: Además de los posibles problemas causados por ataques realizados por personas, es importante tener en cuenta que también los desastres naturales pueden tener muy graves consecuencias, sobre todo si no los contemplamos en nuestra política de seguridad y su implantación, por lo que siempre es recomendable contar con equipos estabilizadores de tensión y, si es posible, que cumplan la función de UPS.
Existen una serie mayor de desastres naturales y alteraciones del entorno que pueden dejar inutilizable la PC, pero consideramos que no deben caer en ésta recomendación debido a que deben haber sido evaluadas para la oficina sobre la que se está ubicado.

- **DEL SOFTWARE**

Independientemente del Sistema Operativo, la primera medida al implementar firma digital, debe ser la definición de cuentas de usuario con contraseña y límites de permisos de administración. La cuenta de administración debe tener una contraseña de exclusivo conocimiento del personal informático responsable de la asistencia técnica.

- **Equipo con Sistema Operativo Windows**
  - Instalación de sistemas Antivirus. Se sugiere contar con el recomendado por la Provincia
  - Sistemas Antispyware. El software para este fin queda a libre elección.
  - Firewall (Cortafuego) (Activar el firewall de windows).
  - Instalar regularmente las actualizaciones de seguridad de windows (por medio de windows Update).
- **Equipo con Sistema Operativo GNU/Linux**
  - Acceder al entorno gráfico del sistema, solamente con usuarios sin privilegios de root (nunca acceder con el usuario root al entorno gráfico).
  - Mantener el sistema actualizado, sobre todo en lo que respecta a las actualizaciones de seguridad.

- **DE LOS DATOS**

Además de proteger el hardware, el entorno y la configuración del software, una política de seguridad mínima, debe contemplar medidas de protección de los datos. Por ello, se considera indispensable, establecer una política adecuada de copias de seguridad, que resguarde los documentos firmados, junto con toda la información necesaria para su posterior validación y recreación del entorno original en el que se produjo la firma, en caso de ser necesario.

FORMULARIOS

Formulario Nº 1 – Jurisdicción y Responsables del Circuito Propuesto

JURISDICCION:

REPARTICIÓN:

AREA/SECCION/DEPARTAMENTO:

NOMBRE DEL CIRCUITO:

FUNCIONARIO RESPONSABLE DEL CIRCUITO

RESPONSABLE DEL PROYECTO (Responsable informático)

Apellido y Nombre:

Lugar de Trabajo:
Teléfonos Directos:
Conmutador: **Internos:**

Correo electrónico (Intranet):

Correo electrónico (Internet):

Firma Responsable

Formulario Nº 2 – Descripción del Circuito Actual

NOMBRE DEL CIRCUITO:

	Area 1	Area 2	Area 3	Area n	Normativa
DESCRIPCION					
FLUJO DE PROCESO					

Formulario Nº 3 – Documentos Involucrados en el Circuito

NOMBRE DEL CIRCUITO:

Nº	Nombre	Descripción	Soporte				Copias del documento		¿Se distribuye?		Observaciones	Otras variables
			Papel		Digital							
			¿Se fotocopia?		¿Se imprime?							
			Si	No	Si	No	Cant.	Frec.	No	Si		
1												
2												
3												

Instrucciones para completar el Formulario Nº 3

Este formulario permite indicar los documentos que circulan por el proceso propuesto y que podrían o no estar sujetos a la aplicación de firma digital. A modo de ejemplo, se pueden citar notas, memos, correos electrónicos, disposiciones, archivos de imágenes, audio y video, etc.

- La primera columna “Nº” es para enumerar correlativamente los documentos involucrados en el circuito y que serán detallados en este formulario.
- La columna “NOMBRE “ es para indicar el nombre del documento.
- En la columna “DESCRIPCION “ se deberá indicar de manera clara y precisa que contenido tiene ese tipo de documento y para qué se utiliza.
- En la columna “SOPORTE” se deberá especificar si el documento esta en formato papel y/o digital, y si el mismo se fotocopia/imprime.
- En “COPIAS DEL DOCUMENTO” indicar la cantidad de veces que el documento es accedido y con qué frecuencia (por hora, diaria, semanal, quincenal, mensual, bimestral, trimestral, semestral, anual, etc, de acuerdo a la variable de medición que el organismo disponga.
- En las columnas siguientes indicar si el documento se imprime y si se distribuye.
- En “OBSERVACIONES” se puede indicar la cantidad de papel involucrado, tiempo, personal y costos de distribución.
- La columna “OTRAS VARIABLES” permite incorporar alguna otra variable que se considere de interés para mostrar la situación actual.

Formulario Nº 4 – Descripción del Circuito Modificado con Firma Digital

NOMBRE DEL CIRCUITO:

	Area 1	**Area 2**	**Area 3**	**Area n**	**Normativa**
DESCRIPCION					
FLUJO DE PROCESO					

Formulario Nº 5 – Análisis de Factibilidad Técnica

JURISDICCION:

REPARTICION:

PROYECTO:

- **OBJETIVO** (describir objetivo general de la propuesta y si corresponde, objetivos particulares)
- **SITUACION ACTUAL** (Describir los elementos que permitan comprender la situación problema que se intenta resolver con la aplicación de firma digital sobre el proceso detallado. Tener en cuenta detallar características de:
  - El proceso
  - Los recursos informáticos
  - Capacitación del personal (Informático y administrativo)

  Presentar medidas que serán visiblemente reducidas con la implementación del proyecto, tales como volúmenes de papel impreso, tiempo ocupado en el proceso o parte de él, cantidad de personas involucradas, tiempo de notificación de documentación, costos asociados, etc.
- **BENEFICIOS** (Describir los resultados esperados teniendo en cuenta la situación problema planteada y las variables que se espera reducir.
- **IMPACTO** (Detallar el impacto que esta aplicación tendrá sobre aspectos informáticos, administrativos y normativos, esto es, indicar tanto las debilidades y/o problemas que podrían presentarse en su desarrollo, tales como resistencias del personal, insuficiente capacitación, equipamiento, falta de apoyo de alguna autoridad, etc. como también las fortalezas que tiene la organización desde esos mismos aspectos)
- **RECURSOS NECESARIOS** (Teniendo en cuenta los puntos detallados anteriormente, estimar las necesidades de equipamiento, capacitación, asesoramiento, afectación de personal, costos, etc.)

Formulario Nº 6 – Detalle de Agentes Autorizados a Utilizar Firma Digital

PROYECTO:

ORGANISMO:

DETALLE DE AGENTES AUTORIZADOS A SOLICITAR CERTIFICADO DIGITAL

REPARTICION	APELLIDO Y NOMBRE	CUIL	CARGO O FUNCION	CORREO ELECTRONICO	TELEFONO

Firma Responsable

Formulario Nº 7 – Solicitud de Revocación de un Certificado Digital

Por la presente, solicito ante la Autoridad de Registro de la Dirección General de Recursos Humanos del Ministerio de Economía de la Provincia de Santa Fe, la revocación del certificado digital vigente, correspondiente a la siguiente persona:

APELLIDO:

NOMBRES:

CUIL:

CARGO:

REPARTICIÓN:

JURISDICCION:

CORREO ELECTRONICO:

Formulario Nº 8 – Solicitud de Dispositivo Criptográfico

JURISDICCION:
REPARTICION:
PROYECTO:
RESPONSABLE DE LA SOLICITUD
APELLIDO Y NOMBRE:
CORREO ELECTRONICO:
TELEFONOS:

ASIGNACION DE TOKENS	
CANTIDAD:	(total de tokens solicitados)
APELLIDO Y NOMBRE	**CUIL**

Firma Responsable

Formulario Nº 9 – Acta de Compromiso – Préstamo de Token

.....(apellido y nombre)....., ...(cargo)....., recibo en este acto el dispositivo criptográfico (TOKEN), para almacenamiento de claves que se utilizarán con **firma digital**, Nº de Serie ....., en calidad de préstamo, sirviendo la presente de formal recibo, y me comprometo a: 1) conservar el mismo, empleando los recaudos necesarios para su mantenimiento y conservación; 2) reintegrarlo en un plazo no mayor a los noventa (90) días a partir de la fecha de la presente; 3) comunicar a la Autoridad de Registro todo cambio o modificación en mi cargo y/o funciones. -

Quedo en conocimiento que ante el incumplimiento de lo dispuesto en este acta, como en lo establecido en la legislación de firma digital, se girarán las actuaciones al área de Asuntos Jurídicos del Ministerio de Gobierno y Reforma del Estado, para su conocimiento y actuación.- - - - - - - - - - - - -

En la ciudad de Santa Fe, a los ..... días de ..... de 20.....-

---

Firma Responsable

Formulario Nº 10 – Registro de Compras de Dispositivos Criptográficos

EXPTE. DE LA GESTION:
L.P./CONC.PRECIOS Nº: **ORDEN PROVISIÓN Nº:**
CANT. DE DISPOSITIVOS: **FECHA RECEPCION:**

DISPOSITIVOS					
TIPO	RECEPCION		ENTREGA		FECHA DEVOLUCION
	Nº INVENTARIO	Nº SERIE	AGENTE	FECHA	
token					
token					
token					
token					
token					
token					
token					
token					
token					
token					
token					
token					
token					
token					
token					
token					
token					
token					
token					

Formulario Nº 11 – Acta Compromiso – Area de Recursos Humanos

Por la presente, ..., DNI ....., Jefe de Área Recursos Humanos de ....., asumo el compromiso de comunicar a la Autoridad de Registro de la Infraestructura de Firma Digital, todo tipo de modificación que se efectúe en el cargo o funciones de los agentes pertenecientes a este organismo a los cuales se les haya emitido un certificado de clave pública a través de la Autoridad de Certificación de la Oficina Nacional de Tecnologías de Información (ONTI).

Firma Responsable

Formulario Nº 12 – Constancia de la Condición de Empleado de una Repartición

....., DNI ....., Jefe de Área Recursos Humanos de ....., en el marco del Proyecto aprobado por la Infraestructura de Firma Digital, dejo constancia de la condición de empleado de esta repartición, de la persona cuyos datos se consignan a continuación:

NOMBRE Y APELLIDO:
DNI:
CUIT:
CARGO:
CATEGORIA: AGRUPAMIENTO:
ESCALFON: SITUACION DE REVISTA:
ORGANISMO:

Certifico que los datos que anteceden son válidos.

Santa Fe, ... de ..... de 20....

Firma Responsable

Formulario Nº 13 – Solicitud de Actividad de Difusión de Firma Digital

Repartición solicitante
Jurisdicción:
Organismo:
Área:
Solicitante
Apellido, Nombre:
Cargo:
Teléfono:
E-Mail:
Tipo de actividad solicitada
Charla ☐ Jornada ☐ Taller ☐ Consulta Personal ☐
Destinatarios
Cantidad estimada:
Perfil (técnico, administrativo, etc):
Objetivos perseguidos con la actividad
Observaciones

Formulario Nº 14 – Recepción De Token

Recibí de ……..(apellido y nombre)……., ……..(cargo)……., el dispositivo criptográfico (TOKEN), Nº de Serie ……., cancelando el préstamo realizado el día …… .

En la ciudad de Santa Fe, a los ……. días de …….. de 20…..-

Firma Responsable

Formulario Nº 15 – Solicitud de Alta de Agente al Sistema SiCAP

SOLICITUD
CUIL:
NOMBRES:
APELLIDO:
TIPO Y NRO DE DOCUMENTO:
CORREO ELECTRONICO (@santafe.gov.ar):
CARGO:
SITUACIÓN DE REVISTA:
TELEFONOS:
JURISDICCION:
REPARTICION:
PROYECTO:

Firma Responsable